VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Bc. Tatiana Hovanová

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

KVANTOVĚ BEZPEČNÁ KRYPTOGRAFIE
QUANTUM-SAFE CRYPTOGRAPHY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Bc. Tatiana Hovanová**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Václav Zeman, Ph.D.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Studentka: Bc. Tatiana Hovanová ***ID:*** 185447
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Kvantově bezpečná kryptografie

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a popište současný stav v oblasti vývoje kvantových počítačů a určete jejich dopad na bezpečnost kryptografických primitiv. Uveďte kvantové algoritmy využívané pro kryptoanalýzu. Určete a souhrnně popište kryptografická schémata, která jsou odolná vůči kryptoanalýze pomocí kvantových algoritmů. Na základě rozboru navrhněte a realizujte výukovou aplikaci, která bude demonstrovat funkci kvantových výpočtů a jednotlivých schémat kvantově bezpečné kryptografie.

DOPORUČENÁ LITERATURA:

[1] BUCHMANN, Johannes, et al. Post-quantum cryptography: lattice signatures. Computing, 2009, 85.1: 105-125.

[2] CHEN, Lily, et al. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology, 2016.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Táto bakalárska práca sa zaoberá možnosťami kvantových výpočtov a ich využitím v kryptoanalytických algoritmoch. Úvodné kapitoly sú venované vysvetleniu základných pojmov z oblasti kvantovej teórie a kvantových operácií. Časť práce opisuje javy, ktoré ovplyvňujú splnenie DiVincenzových kritérií ako napríklad superpozícia, kvantové previazanie, interferencia, dekoherencia a kvantová korekcia chýb. Kapitola venovaná súčasným kvantovým počítačom rozoberá aktuálny stav vývoja kvantového počítača firmami IBM, D-Wave a Intel. Z kryptoanalytických algoritmov je bližšie popísaný Shorov a Groverov algoritmus, pričom je uvedený aj ich dopad na bezpečnosť. Postkvantová kryptografia je reprezentovaná kryptosystémami zo štyroch základných smerov: kryptografia založená na hashoch (Lamportova schéma, Merklova schéma), kryptografia založená na teórií kódovania (kryptosystém McEliece), kryptografia založená na mriežkach (NTRU kryptosystém) a kryptografia založená na polynomiálnych rovniciach (prúdová šifra QAUD). Ďalšia časť práce je venovaná návrhu výukovej aplikácie formou webu, ktorý okrem iného obsahuje laboratórne úlohy demonštrujúce aktuálne možnosti kvantových obvodov. Webová stránka formou animácií vysvetľuje princípy vybraných operácií, kryptosystémov a algoritmov. Prvá laboratórna práca sa zaoberá úvodom do kvantových výpočtov. Obsahuje päť čiastkových úloh vysvetľujúcich základne kvantové operácie (Hadamard, X-rotácia, Z-rotácia, Y-rotácia a pod.). Druhá laboratórna úloha obsahuje návod na konštrukciu Groverovho algoritmu pomocou simulátoru Quirk.

KĽÚČOVÉ SLOVÁ

Kvantová kryptografia, kvantové počítanie, Quirk, Shorov algoritmus , Groverov algoritmus

ABSTRACT

This bachelor thesis deals with the possibilities of quantum computatutions and their use in cryptanalytic algorithms. The introductory chapters are devoted to explaining the basic concepts of quantum theory and quantum operations. Part of the thesis describes effects, that affect DiVincenzo's criteria, such as superposition, quantum entanglement, quantum interference, decoherence, and quantum error correction. The current quantum computer chapter deals with the current stage of the quantum computer development by IBM, D-Wave and Intel. Shor's and Grover's algorithm are described from cryptoanalytical algorithms, and their impact on security is also described. Post-quantum cryptography is represented by cryptosystems from four basic directions: hash-based cryptography (Lamport's scheme, Merkle's scheme), cryptography based on coding theory (McEliece cryptosystem), grid-based cryptography (NTRU cryptosystem) and cryptography based on polynomial equations (stream cipher QAUD). The next part of the thesis is devoted to the design of a web-based educational application that includes, among other things, laboratory tasks demonstrating the current possibilities of quantum circuits. The website explains the principles of selected operations, cryptosystems and algorithms in the form of animations. The first laboratory task deals with the introduction to quantum computations. It contains five partial tasks explaining the basics of quantum operation (Hadamard, X-rotation, Z-rotation, Y-rotation, etc.). The second task includes instructions for constructing the Grover's algorithm using the Quirk simulator.

KEYWORDS

Quantum cryptography, quntum computation, Quirk, Shor's algorithm, Grover's algorithm

HOVANOVÁ, Tatiana. *Kvantově bezpečná kryptografie*. Brno, 2019, 61 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: doc. Ing. Václav Zeman, Ph.D.

VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Kvantově bezpečná kryptografie“ vypracovala samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autora uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušila autorské práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomá následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autorky

POĎAKOVANIE

Moja vďaka patrí vedúcemu bakalárskej práce pánovi doc. Ing. Václavovi Zemanovi Ph.D. za odborné vedenie, konzultácie a za cenné a odborné poznámky k práci. Ďalej patrí moje poďakovanie rodine, ktorá má nie len počas písania práce, ale aj počas celého štúdia podporovala.

Brno . . . .

podpis autorky

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Táto práca sa zaoberá možnosťami kvantových počítačov a to od ich úplných základov (kvantové počítanie), cez kryptoanalytické algoritmy až po post-kvantovú kryptografiu, čo je označenie pre kryptografiu, ktorá je odolná voči kvantovým výpočtom.

Obor kvantových počítačov zažíva v súčasnosti veľký rozmach a to najmä kvôli tomu, že veľkosť súčiastok konvenčných počítačov sa natoľko zmenšila, že ich ďalšia miniaturizácia nebude možná bez toho, aby sa nezačali uplatňovať kvantové zákony. Využitie kvantových častíc však so sebou prináša radu nevýhod, s ktorými sa vedci musia najprv vyrovnať do takej miery, aby bolo možné kvantový počítač reálne skonštruovať. Tejto problematike sa venuje kapitola 4 a 5.

V súčastnosti už existuje viacero kryptoanalytických algoritmov pracujúcich s kvantovým počítačom v teoretickej rovine. Azda najzásadnejšími sú Shorov algoritmus a Groverov algoritmus (kapitola 6). Tieto algoritmy vyústia v to, že ak sa vedcom podarí zostrojiť dostatočne efektívny kvantový počítač, bude to znamenať koniec mnohých dnes využívaných kryptografických algoritmov založených na probléme diskrétneho logaritmu alebo na faktorizačnom probléme. Kvantové počítače rovnako budú hrať úlohu pri veľkosti kľúčov symetrických algoritmov – vyžiadajú zdvojnásobenie dĺžky kľúča pre rovnaké zabezpečenie, ako dosahujú pri konvenčných počítačoch. Vzhľadom k tejto skutočnosti začali viacerí vedci pracovať na algoritmoch, ktoré budú odolné voči kvantovým výpočtom. Vznikli tak štyri základné smery, ktorými sa uberá post-kvantová kryptografia – kryptografia založená na hashoch, kryptografia založená na teórii kódovania, kryptografia založená na mriežkach a kryptografia založená na polynomiálych rovniciach. Tejto problematike je venovaná kapitola 7.

Posledná časť tejto práce sa zaoberá vytvorením webovej výukovej aplikácie. Tá je orientovaná na teoretický výklad doplnený animáciami vybraných algoritmov či operácií. Nezanedbateľnú časť aplikácie tvoria dve laboratórne úlohy zamerané na objasnenie základných kvantových operácií a tiež na praktickú demonštráciu Groverovho algoritmu v kvantovom simulátore Quirk.

1 Kvantové počítanie

Klasická teória informácie pracuje s bitmi, ktoré predstavujú dvojstavový systém so stavmi 0 a 1. Združovaním bitov dokážeme reprezentovať ľubovolnú časť informácie. Ekvivalentnými základnými stavebnými prvkami kvantovej informácie sú kvantové bity zvané qubity. Qubit je systém s dvomi ortogonálnymi základnými stavmi, ktoré sa označujú ako $|0\rangle$ a $|1\rangle$ (Off a On). Existuje množstvo fyzikálnych implementácií qubitu (viac v kapitole č.3) ako napríklad polarizácia fotónu či spin elektrónu [1, str. 10-15].V matematickej reprezentácii však nie je konkrétna implementácia podstatná – postačuje, ak sa jedná o dvojhladinový Hilbertov systém.

Kvantové počítanie môžeme podľa Scotta Aaronsona popísať analogicky ako teóriu pravdepodobnosti, s tým rozdielom, že pracuje s komplexnými číslami [2]. **Pravdepodobnostný systém** je systém, kde funkcia P každému javu A z výberového priestoru, priraďuje reálne číslo $P(A)$ nazývané pravdepodobnosť. Súčet všetkých pravdepodobností stavov výberového priestoru je rovný 1[3].

Príklad: Máme mincu, ktorou hádžeme, pričom vždy padne hlava alebo orol. Pokiaľ minca nespadne a my nevieme výsledok, tak výsledok (a celý systém) sa nachádza v stave (hlava 0,5; orol 0,5). V prípade, že minca spadla a my sme zistili, že padol orol, tak výsledok sa nachádza v stave (hlava 0, orol 1). V oboch prípadoch dostávame po sčítaní možných stavov 1.

Kvantový systém sa správa analogicky, avšak funkcia P, priraďuje javom namiesto reálneho čísla číslo komplexné. Komplexné číslo (a teda aj qubit) sa dá vyjadriť v tvare $ai + b$, kde a a b sú reálne čísla, i je výsledok $x^2 = -1$ a nazýva sa aj imaginárne číslo. Komplexné číslo môžeme popísať tromi charakteristikami: fáza, amplitúda pravdepodobnosti a veľkosť komplexného čísla. **Fáza** je pre každé komplexné číslo zapísané v polárnych súradniciach $|r|e^{i\varphi}$ rovná $e^{i\varphi}$, kde $|r|$ predstavuje veľkosť komplexného čísla. Fáza nemá sama o sebe žiadny fyzikálny význam. **Amplitúda pravdepodobnosti** je v kvantovej mechanike komplexné číslo priradené neurčitému stavu, ktoré nie je možné priamo merať. Pravdepodobnosť, že daný stav nastane, je definovaný ako štvorec absolútnej hodnoty amplitúdy pravdepodobnosti. Amplitúda poskytuje vzťah medzi stavovým vektorom a výsledkami pozorovania tohto systému. **Veľkosť** komplexného čísla môžeme počítať ako veľkosť vektora v Gaussovej rovine [2]: $r = |x^2 + y^2|$.

Príklad: Máme kvantovú mincu, ktorou hádžeme, pričom vždy padne hlava alebo orol. Pokiaľ minca nespadne a my nevieme výsledok, tak výsledok (a celý systém) sa môže nachádzať napríklad v stave (hlava: $1/\sqrt{2}$; orol $1/\sqrt{2}$) a v množstve iných.

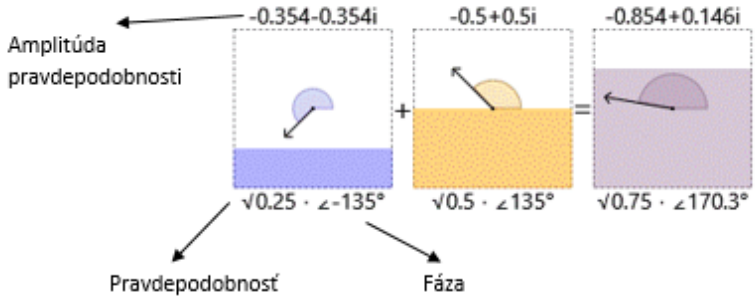
Všetky stavy kvantového systému je možné popísať vektorom z Hilbertovho priestoru. Hilbertov priestor je úplný vektorový priestor so skalárnym súčinom, ktorý indukuje normu a metriku. Najjednoduchší kvantový objekt kvantovej teórie informácie je qubit popísaný práve dvojrozmerným Hilbertovym priestorom. Dvojhladinový systém je možné zapísať ako:

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{1.0.1}$$

kde c_1 a c_2 sú komplexné čísla, vyjadrujúce amplitúdu pravdepodobnosti spĺňajúce podmienku $|c_1|^2 + |c_2|^2 = 1$. Vektor $[1,0]^\intercal$ sa značí $|0\rangle$, $|1\rangle$ je označenie pre vektor $[0,1]^\intercal$.

Poznámka: Zátvorky pri 0 a 1 značia takzvanú Diracovu notáciu. Ak máme vektor (a,b), tak ho môžeme zapísať ako $\alpha|0>$ a $\beta|1>$, kde α je amplitúda stavu $|0\rangle$ a β je amplitúda stavu $|1\rangle$.

Richard Feynman uviedol na svojej prednáške inú grafickú reprezentáciu – tá zobrazuje fázu, amplitúdu a veľkosť komplexného čísla zároveň (viď. obr. 1.1). Osa X predstavuje reálnu časť komplexného čísla, osa Y imaginárnu časť komplexného čísla, „rotujúca šípka“ zobrazuje hodnotu amplitúdy, veľkosť je reprezentovaná dĺžkou šípky. Fázu je možné zobraziť pomocou uhlu. Keďže štvorec amplitúdy určuje pravdepodobnosť stavu, je zobrazený podielom naplnenej plochy štvorca [4].



Obr. 1.1: Grafická reprezentácia komplexného čísla

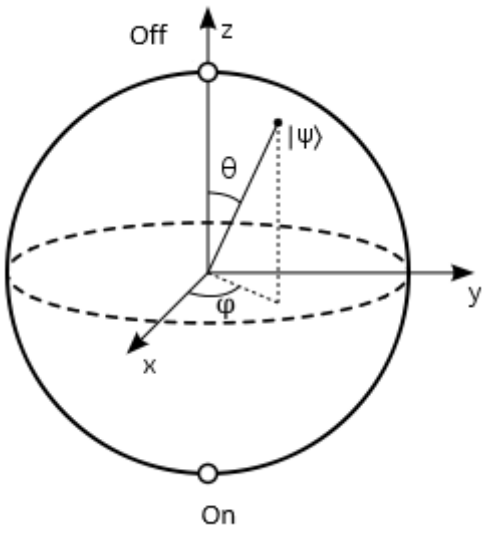
1.1 Grafická reprezentácia qubitu

Ako bolo uvedené v predchádzajúcej kapitole, qubity je možné reprezentovať pomocou vektorov v dvojrozmernom priestore. Avšak často sú qubity reprezentované

pomocou tzv. Blochovej sféry, ktorá predstavuje trojrozmerné zobrazenie. Uvažujeme všeobecný kvantový stav $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$, kde c_1, c_2 sú komplexné čísla. Použitím polárnej reprezentácie môžeme vytvoriť ekvivalentnú reprezentáciu:

$$|\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle, \tag{1.1.1}$$

kde uhol θ a φ môže nadobúdať hodnoty $\theta \in [0, \pi)$, $\varphi \in [0, 2\pi)$, tak aby pokryli celú sféru bez opakovania. Póly Blochovej sféry reprezentujú bázové vektory $|0\rangle$, $|1\rangle$; všeobecné stavy pokrývajú celú plochu sféry. Uhol θ vyjadruje pravdepodobnosť namerania stavu Off – ak sa stav nachádza „bližšie“ k severnému pólu je pravdepodobnejšie, že pri meraní všeobecný stav skolabuje do bázového stavu Off. Ak sa stav nachádza priamo na rovníku, existuje pravdepodobnosť 0,5, že pri meraní skolabuje do stavu On a pravdepodobnosť 0,5, že skolabuje do stavu Off. Na druhú stranu, rotácia okolo osy z vyústi do fázového posunu, čo pri meraní žiadnym spôsobom neovplyvní stav, do ktorého qubit skolabuje. Táto rotácia je reprezentovaná zmenou uhlu φ [5] .



Obr. 1.2: Blochova sféra

2 Príklady kvantových logických funkcií

Vo všeobecnosti existuje množstvo kvantových operácií. Ich základnou vlastnosťou je **reverzibilnosť**, čo znamená že pokiaľ aplikuje kvantovú operáciu U na vstupný stav $|\psi\rangle$ a dostaneme výstupný stav $U|\psi\rangle$, vždy môžeme aplikovať inverznú operáciu U^T, čím získame pôvodný stav $|\psi\rangle$. Dôsledok tejto vlastnosti je ten, že operácia NOT môže byť implementovaná analogicky ako pri bežných operáciach, čo nie je možné uskutočniť pre operácie AND a OR. Dôvod je nasledujúci. Klasická operácia NOT (pre vstup 0 je na výstupe 1, pre vstup 1 je na výstupe 0) mapuje výstup jednoznačne. Znamená to, že pokiaľ máme na výstupe 1, dokážeme jednoznačne rozhodnúť, aký stav bol na vstupe. Pre operáciu AND nedokážeme takúto spätnú rekonštrukciu jednoznačne vykonať. Pokiaľ dostaneme na výstupe 0, vstupom mohli byť bity 0 a 1, ale zároveň 0 a 0. Operácia AND (rovnako ako OR) nie je reverzibilná, preto nemôže byť jednoducho implementovateľná pomocou kvantových operácií. Pri zostrojovaní týchto operácií sa využívajú kvantové operácie CSWAP, CNOT a NOT (pre viac detailov odkážme čitateľa na literatúru [6]).

2.1 Pauliho operácie

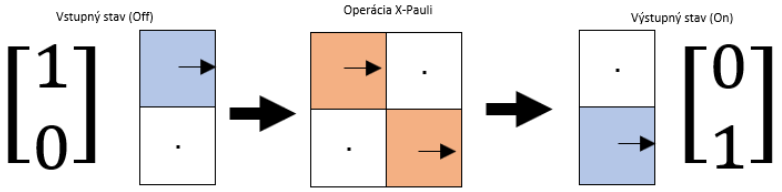
Existujú celkom tri Pauliho operácie – X-operácia, Y-operácia a Z-operácia. Svoje názvy nesú podľa toho, akú rotáciu predstavujú v Blochovej sfére (napr. X-operácia je rotácia okolo osi x o 180°). Existujú aj verzie operácií predstavujúce rotácie o 90°, −90°, 45°, −45°, 22.5° a −22.5°.

2.1.1 Pauliho X-operácia

Základnou kvantovou logickou funkciou je Pauliho X-operácia aplikovaná na jeden kvantový stav, čo predstavuje kvantovú obdobu operácie NOT. Funkciou tejto operácie je zmeniť kvantový stav Off na On a On na Off (inak povedané stav $|0\rangle$ na $|1\rangle$ a stav $|1\rangle$ na stav $|0\rangle$). Operácia odpovedá násobeniu zľava maticou (podľa [7]):

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.1.1}$$

Dobrú predstavu o tom, ako táto operácia funguje je možné si vytvoriť na základe obrázku č. 2.1, ktorý je vytvorený pomocou Feynmanového zápisu. Ako môžeme vidieť, operácia neovplyvňuje amplitúdu pravdepodobnosti daného stavu.



Obr. 2.1: Grafické zobrazenie prechodu stavu Off Pauliho-X operáciou

Príklad: Ako príklad uvedieme aplikáciu Pauliho X-operácie na stav On. $|1\rangle$ je v maticovom zápise

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{2.1.2}$$

a teda

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \cdot 1 + 1 \cdot 1 \\ 0 \cdot 1 + 1 \cdot 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \tag{2.1.3}$$

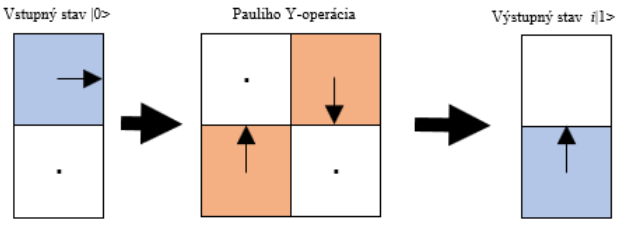
čo odpovedá $|0\rangle$ (Off stav).

2.1.2 Pauliho Y-operácia a Z-operácia

Pauliho Y-operácia predstavuje rotáciu okolo osi y o 180° v Blochovej sfére. Maticové vyjadrenie operácie je (podľa [7]):

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2.1.4}$$

Operácia prevádza stav $|0\rangle$ na stav $i\,|1\rangle$, stav $|1\rangle$ na stav $-i\,|0\rangle$.

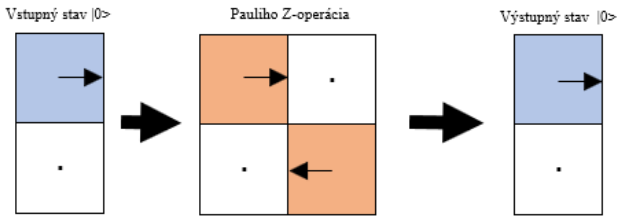


Obr. 2.2: Grafické zobrazenie prechodu stavu Off Pauliho-Y operáciou

Pauliho Z-operácia predstavuje rotáciu okolo osi z o 180° v Blochovej sfére. Maticové vyjadrenie operácie je (podľa [7]):

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.1.5}$$

Operácia prevádza stav $|0\rangle$ na stav $|0\rangle$, stav $|1\rangle$ na stav $-|1\rangle$.

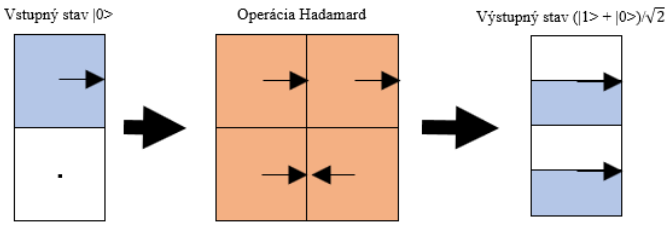


Obr. 2.3: Grafické zobrazenie prechodu stavu Off Pauliho-Z operáciou

2.2 Operácia HADAMARD

Operácia Hadamard je verziou kvantovej Fourierovej transformácie nad jedným qubitom. Operácia je zodpovedná za vytvorenie superpozície nad kvantovými stavmi, čo znamená, že Off stav je prevedený do stavu (Off+On)/$\sqrt{2}$ a On stav do stavu (Off-On)/$\sqrt{2}$. Operácia odpovedá násobeniu maticou (podľa [7]):

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}. \tag{2.2.1}$$



Obr. 2.4: Grafické zobrazenie prechodu stavu Off operáciou Hadamard

Príklad: Aplikujeme v dvoch iteráciach operáciu Hadamard na stav $|1\rangle$ (On stav).

Prvá iterácia:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\cdot\begin{bmatrix}0\\ 1\end{bmatrix}=\begin{bmatrix}0\cdot\frac{1}{\sqrt{2}}+1\cdot\frac{1}{\sqrt{2}}\\ 0\cdot\frac{1}{\sqrt{2}}-1\cdot\frac{1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}. \tag{2.2.2}$$

Pre vyjadrenie v Diracovej notácií postupne upravujeme:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.2.3}$$

Druhá iterácia:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}} \cdot = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \tag{2.2.4}$$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \cdot \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \cdot \left(\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} \right) \cdot = \tag{2.2.5}$$

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \cdot \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.2.6}$$

Čím sme práve ukázali, že operácia Hadamard je reverzibilná.

3 Fyzikálna implementácia kvantového systému

Ako už bolo spomínané, qubit môže byť realizovaný pomocou ľubovoľného kvantového dvojstatového systému. Bližšie bude predstavená implementácia pomocou Josephsonovho efektu, ktorý využíva kvantový počítač IBM Q, potom polarizácia fotónu a spin elektrónu, ktoré sa často prezentujú pri demonštrácií kvantových výpočtov.

3.1 Josephsonov efekt – fázový qubit

Fázový qubit využíva počítač IBM Q, kde má qubit fyzikálnu podobu Josephsonovsovho spoja. Dva kusy supravodivého kovu sú oddelené tenkou izolačnou bariérou tak, aby páry elektrónov mohli tunelovať izolant. Prúd tečúci Josephsonovým spojom je možné vyjadriť ako $I = I_0 \sin \delta$, kde δ je rozdiel fáz komplexných vlnových funkcií popisujúcich supravodivé stavy na stranách spoja. Hodnota fázového posunu δ sa snaží zaujať buď najnižšie minimum potenciálu valchy alebo prvý excitovaný stav – to znamená, že systém sa môže dostávať do dvoch stavov. Pri udržaní niekoľkodňovej nízkej teplote (15 mK) sa dostáva supravodivý fázový qubit do rovnováhy tj. základného stavu $|0\rangle$. Aplikáciou operácie NOT sa qubit s vysokou pravdepodobnosťou dostane do stavu $|1\rangle$ [8].

3.2 Fotón – polarizácia

V prípade reprezentácie qubitu pomocou polarizácie môžeme povedať, že stav $|0\rangle$ bude prezentovaný horizontálnou polarizáciou a stav $|1\rangle$ polarizáciou vertikálnou. Problémom tejto reprezentácie je fakt, že polarizácia sa mení pri šírení prostredím napr. vzduchom či optickým káblom. Polarizácia je fyzikálna veličina, ktorá udáva v akom smere svetlo osciluje (kmitá). Polarizačný filter je materiál prepúšťajúci svetlo s určitou polarizáciou. Polarizácia sa vzťahuje aj na fotóny (majú frekvenciu, hybnosť a polarizáciu). Ak postavíme za sebou dva polarizačné filtre (bázi) pootočené o 90° tak fotón, ktorý prejde cez prvý filter, sa nachádza v stave ňom určenom – môže to byť napríklad horizontálny stav. Pri prechode druhým vertikálnym filtrom fotón neprejde. Ak však zmeníme otočenie prvého filtra (do inej roviny ako kolmo k druhému filtru), tak fotón druhým filtrom niekedy prejde a niekedy nie (závisí to na amplitúde) – prvý filter teda „znáhodnil“ meranie na druhom filtre [8].

3.3 Elektrón – spin

Každý makroskopický objekt môže mať moment hybnosti vyjadrujúci mieru pohybu vzhľadom k určitému miestu. V prípade, kedy je objekt nabitý, vytvára tento pohyb magnetické pole. Spin je ďalšia vlastnosť elementárnych objektov, ktorá sa skladá s momentom hybnosti. Spin sa označuje ako vnútorný stav hybnosti, pričom nie je možné si ho nejak predstaviť. Spin dokážeme merať u elementárnych objektov vďaka magnetickému poľu, ktoré generuje, a to narozdiel od momentu hybnosti makroskopických objektov aj v prípade, že objekty nie sú nabité. Magnetický moment môže byť orientovaný dvoma smermi, čo môžeme interpretovať ako $|0\rangle$ (spin hore) a $|1\rangle$ (spin dole). Meranie môžeme uskutočniť napríklad preletom elementárneho objektu nehomogénnym magnetickým poľom. Objekt so spinom hore sa vychýli na jednu stranu, pričom objekt so spinom dole sa vychýli na stranu opačnú [9].

4 Javy ovplyvňujúce konštrukciu kvantového počítača

DiVincenzové kritéria tvoria zoznam podmienok, ktoré sú nevyhnutné pre dobre zostrojený kvantový počítač:

- fyzikálny systém musí dobre charakterizovať qubity,
- systém musí byť schopný inicializovať východzí stav a dostatočne dlho ho udržať,
- musí existovať univerzálna sada kvantových operácií,
- systém musí byť schopný zmerať stav qubitov,
- systém musí mať dlhú koherenčnú dobu [10].

V kvantovej mechanike existujú fundamentálne princípy, ktoré ovplyvňujú správanie každého kvantového počítača tj. ovplyvňujú splnenie DiVincenzových kritérií. Zjednodušene môžeme povedať, že kvantový počítač využíva tri základné kvantové princípy: superpozíciu, interferenciu a kvantové previazanie. Taktiež je dôležité brať v úvahu, že existujú určité obmedzenia, ktoré v reálnom svete negatívne determinujú možnosť zostrojenia univerzálneho kvantového počítača. Takéto obmedzenia môžu byť spojené s meraním kvantových stavov, dekehorenciou či kvantovou korekciou chýb.

Kvantové previazanie je definované ako systém, kde sú objekty spojené tak, že jeden objekt nie je možné úplne popísať bez popisu jeho dvojice a to i v prípade, že sú objekty od seba priestorovo oddelené. Práve kvantové previazanie je z veľkej časti zodpovedné za vysoký výpočtový výkon kvantových počítačov, pretože informácia je paralelne nesená o všetkých stavoch superpozície. Ak previažeme n qubitov do registru, superponovaný systém sa môže nachádzať v jednej chvíli v 2^n stavoch [11].

Pri opise správania kvantového počítaču nemôžeme opomenúť jav zvaný **interferencia**. Ten vychádza z faktu, že pravdepodobnosť je nezáporná a môže sa len sčítať, ale amplitúda môže byť nezáporná ale aj záporná. V tom prípade sa dá aj odčítať, to znamená, že dve amplitúdy sa môžu navzájom vyrušiť [12].

Predpokladajme jeden qubit. Začneme v qubite $|0\rangle$ a aplikujeme na neho operáciu Hadamard:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{4.0.1}$$

čím dostávame qubit do superpozície. Ak aplikujeme transformáciu po druhý krát dostávame:

$$H\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{H|0\rangle + H|1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle + |0\rangle - |1\rangle}{\sqrt{2}} = |0\rangle, \tag{4.0.2}$$

tj. výsledkom je pôvodný stav $|0\rangle$. Ako môžeme vidieť v poslednom kroku, amplitúdy stavu $|1\rangle$ interferovali deštruktívne – veľkosť bola rovnaká, ale mala opačné znamienko. Z tohto dôvodu sa vo výsledku stav $|1\rangle$ nevyskytuje. Na druhej strane, amplitúdy $|0\rangle$ interferovali konštruktívne.

Interferencia úzko súvisí so **superpozíciou** a možnosťou kvantového merania. Superpozíciou môžeme nazvať vlastnosť kvantového systému, kedy sa systém súčasne nachádza vo viacerých stavoch, až pokiaľ nebude vykonané meranie. V skutočnosti to znamená, že superpozícia nikdy nebude môcť byť nameraná, pretože ju meranie naruší [2].

Ak prevedieme **meranie** v superpozícii $\alpha|0\rangle + \beta|1\rangle$, mali by sme dostať odpoveď: $|0\rangle$ s pravdepodobnosťou α^2 a $|1\rangle$ s pravdepodobnosťou β^2. Pri meraní ale nastáva deštruktívna interferencia, a teda pokiaľ qubit nie je v bázovom stave $|0\rangle$ alebo $|1\rangle$, vyberie sa jedna z odpovedí $|0\rangle$ s pravdepodobnosťou α^2 a $|1\rangle$ s pravdepodobnosťou β^2[2].

K tomu aby bolo možné udržať kvantový stav je nutné kvantový systém izolovať od okolia, čo nie je v reálnych podmienkach jednoduché. Ak systém nie je izolovaný, nastane dekoherencia, čo je je proces narušenia vlastností potrebných pre kvantovú superpozíciu. **Dekoherencia** vzniká tým, že objekty sú v kontakte s okolím, ktoré ruší kvantovú superpozíciu stavov [2].

Korekcia chýb pri bežných počítačoch využíva nadbytočnosť pri ochrane informácií pred chybami spôsobenými šumom pri prenose. Jedným z možných spôsobov korekcie chýb, je uloženie informácie viacero krát. Ak niektorá z kópií informácie nesúhlasí s ostatnými, použijeme tú informáciu, ktorá sa vyskytuje najviac krát. Tento princíp však nie je možné využiť pri kvantových počítačoch kvôli tzv. no-cloning teorému, ktorý tvrdí, že ľubovoľný neznámy kvantový stav nie je možné identicky skopírovať. Peter Shor však dokázal, že je možné uchovať informáciu o jednom qubite prostredníctvom ostatých qubitov a to vďaka kvantovému previazaniu [13]. Počet použitých qubitov ovplyvňuje pravdepodobnosť, že qubit bude reprezentovať správnu hodnotu. Správny výsledok by sme so 100% pravdepodobnosťou dosiahli, ak by systém obsahoval nekonečne qubitov.To by prakticky znamenalo zostrojiť nekonečný kvantový register, čo nie je možné. Kvôli tomu môžeme trdiť iba to, že qubit reprezentuje danú hodnotu s určitou pravdepodobnosťou, pričom je snaha dosiahnuť túto pravdepodobnosť čo najväčšiu [2].

5 Súčasné kvantové počítače

Súčasné kvantové počítače pracujú v komerčnej verzii maximálne s 20 qubitmi (stav k 30.11.2018), pričom vedci odhadujú, že pri približne 100 qubitoch bude kvantový počítač schopný robiť výpočty (pre obmedzené typy úloh) predstavujúce pre dnešné počítače problém [14]. Veľmi dôležitým problémom v oblasti kryptografie je faktorizačný problém, na ktorý je možné previesť problém diskrétneho algoritmu aj problém diskrétneho algoritmu prvku eliptickej krivky (viac v kapitole 6). Pomocou kvantového počítača od IBM bolo faktorizované číslo 4 088 459 použitím 2 qubitov z 5-qubitového a 16-qubitového procesoru, pričom nebol využitý Shorov algoritmus ale špeciálny postup vyvinutý iba pre toto číslo a číslo 56 153 [15]. Všeobecným Shorovým algoritmom bolo faktorizované číslo 21 [16]. Pre porovnanie uveďme, že v súčasnej dobe bolo klasickým počítačom faktorizované číslo $2^n - 1$, kde n = 1193.

5.1 IBM

IBM začalo verejne pracovať na kvantovom počítači v roku 2016, kedy došlo k demonštrácií IBM Q Experience – prototypu kvantovej výpočtovej techniky pracujúcej online. Vznikla tak prvá platforma spájajúca možnosti cloudu a kvantového počítača [17]. Následne na to, v roku 2017, vzniká spoločnosť IBM Q – komunita 500 spoločností, startupov, akademických inštitúcií, národných výskumných laboratórií spolupracujúcich s IBM v oblasti kvantovej výpočtovej techniky. Cieľom tohto partnerstva je urýchlenie pokroku objavovania prvých kvantových aplikácií [18]. 17.mája 2017 oznámila spoločnosť IBM, že úspešne vybudovala a otestovala dva procesory umožňujúce kvantové výpočty IBM využíva v QPU (Qunatum Processing Unit) Josephsonov spoj [19].

Prvý procesor vznikol inováciou už existujúceho 5-qubitového procesoru na 16-qubitový. Bol vytvorený pre účely skúmania kvantovej techniky vývojármi, programátormi a výskumníkmi. Bezplatný prístup je možný skrz webové rozhranie IBM Cloudu [19]. V súčasnej dobe je pre vedecké účely dostupný 14-qubitový procesor v Melbourne, 16-qubitový procesor v Rüschlikon a 5-qubitový procesor v Tenerife [20].

Druhý procesor bol prototyp vyvinutý pre vznikajúci kvantový komerčný systém. Dokázal pracovať so 17-qubitmi a bol navrhnutý tak, aby bol najmenej dvakrát účinnejší ako verejný kvantový procesor pre výskumné účely. Tento prototyp bol konštruovaný z vylepšených materiálov, zariadení a vylepšením prešla aj architektúra procesoru [19].Od uvedenia na trh v roku 2017 bol inovovaný na 20-qubitový a je umiestnený v Tokiu [21].

Koncom roku 2017 IBM predstavilo svoj doposiaľ najvýkonnejší kvantový procesor pracujúci s 50-qubitmi. Spoločnosť označuje tento úspech za významný medzník v pokroku smerom k praktickým kvantovým počítačom. Iné doteraz vybudované systémy mali obmedzené výpočtové vlastnosti, to znamená, že zvládali vykonávať výpočty, ktoré zvládal aj konvenčný počítač. Práve 50-qubitov predstavuje hranicu, kedy stroj dokáže vykonávať výpočty, ktoré sú extrémne ťažké bez kvantovej technológie [21].

Okrem toho IBM vytvorila **simulátor** kvantového procesoru. Jedná sa o prostredie navrhnuté pre vývojárov kvantových software skúšajúcich možnosti reálneho kvantového hardware. Simulátor pracuje s 32-qubitmi [20].

Využitie kvantových výpočtov vidí IBM v :
-*„**podniková optimalizácia**: riešenie komplexných problémov v dodávateľských reťazcoch, logistike, modelovaní finančných údajov a analýze rizík;*
- ***materiály a chémia**: riešenie molekulárnych a chemických interakcií vedúcich k objavovaniu nových materiálov a liekov;*
- ***umelá inteligencia**: efektívne vytváranie umelej inteligencie ako napríklad strojového učenia;*
- ***cloudová bezpečnosť**: používanie zákonov kvantovej fyziky na zvýšenie bezpečnosti súkromných dát v cloude [19].“*

5.2 Intel

V roku 2017 predstavil Intel postupne 7, 17 a 49-qubitový chip. 49-qubitový čip je pomenovaný podľa jazier v Aliaške Tangle Lake. Jedná sa o referenciu na extrémne nízku teplotu, ktorú procesor potrebuje k funkcii. Rovnako ako chip od IBM aj Intel využíva supravodivé obvody [22]. Čip pozostáva zo 108 konektorov rádiovej frekvencie, ktoré prenášajú mikrovlnný signál do čipu, ktorý organizuje qubity. Každý nióbový qubit pozostáva z dvoch tunelov, ktoré sú tvorené dvomi tenkými oxidovými filmami medzi dvoma vodičmi, čím vytvárajú Josephsonov spoj [23].

V júni roku 2018 začala spoločnosť testovať inú technológiu – procesor založený na báze kremíka pracujúci so spinom. Spinové qubity fungujú na základe spinu jedného elektrónu v kremíku, riadeného mikrovlnnými pulzmi. Výhodou tohto riešenia je, že spinové qubity sa oveľa viac podobajú konvenčným polovodičovým súčiastkam, čo umožňuje využiť existujúce výrobné techniky. Spinové qubity, tak isto ako supravodivé qubity, vyžadujú extrémne nízku teplotu avšak v nižšej miere (jeden kelvin oproti 20 milikelvinov). Vedci z Intelu očakávajú, že spinové qubity dokážu byť v koherentnom stave dlhšiu dobu ako supravodivé, čo je možné s výhodou využiť

pri implementácií kvantových algoritmov. Spinové qubity zaberajú menší priestor – teoreticky je možné miliardu spinových qubitov zmestiť na štvorcový milimeter plochy. V kombinácií s ich podobnosťou s konvenčnými polovodičovými súčiastkami, by táto technológia mohla viesť k zvyšovaniu počtu qubitov, s ktorými sú kvantové systémy schopné pracovať [24].

5.3 D-Wave

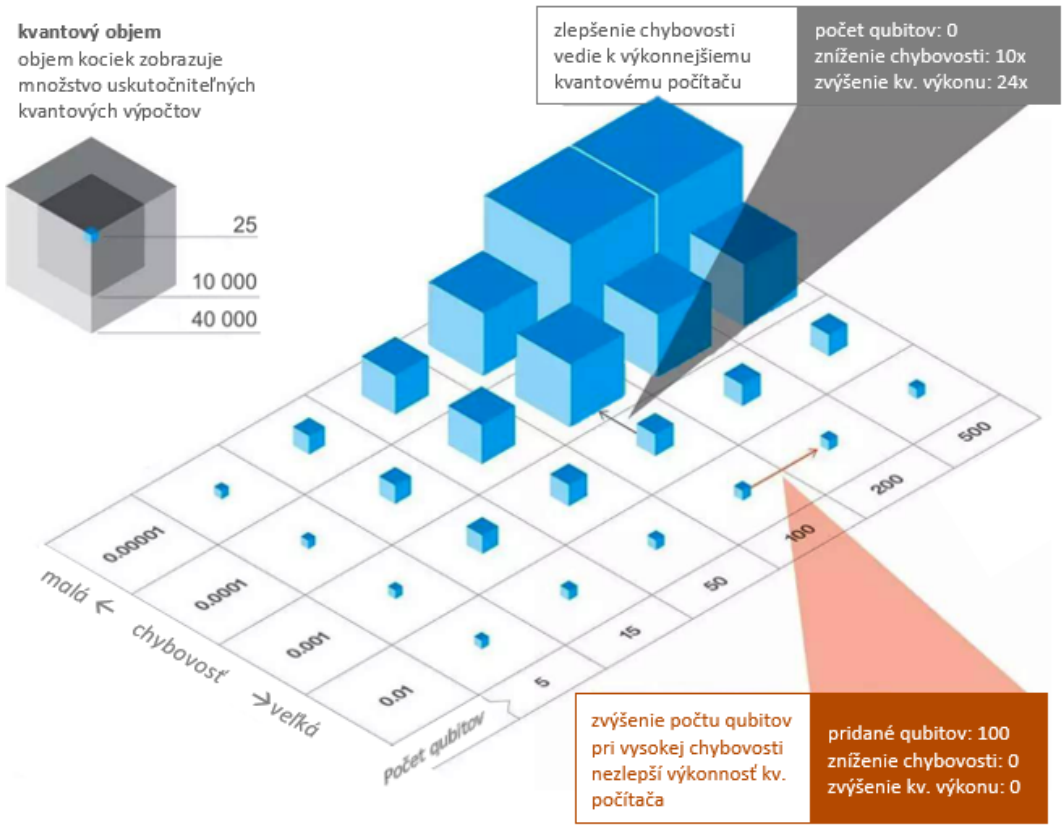
D-Wave bola prvou spoločnosťou na svete, ktorá predávala počítače využívajúce kvantové výpočty. Najnovší počítač D-Wace 2000Q dokáže pracovať až s 2048 qubitmi a podľa údajov od spoločnosti D-Wave je tisíckrát výkonnejší, ako predchádzajúci model (D-Wave 2X). Obvody v QPU dokážu konfigurovať magnetické pole, vďaka čomu je možné čip programovať [25]. Čip pracuje na základe kvantového žíhania, čo obmedzuje jeho použitie – funguje len pre adiabatické kvantové výpočty čo je typ výpočtu, ktorý rieši optimalizačnú úlohu. Optimalizačná úloha je zameraná na nájdenie vyhovujúceho riešenia parametrickej úlohy. Riešiť takúto úlohu znamená hľadať globálny extrém na krivke tj. prehľadávať stavový priestor.

	D-Wave One	D-Wave Two	D-Wave 2X	D-Wave 2000Q
Dátum uvedenia	máj 2011	máj 2013	august 2015	január 2017
Počet qubitov	128	512	1152	2048
Kúpený spoločnosťou	Lockheed Martin	Lockheed Martin, NASA, USRA, Google	Lockheed Martin, NASA, USRA, Google, Los Alamos National Laboratory	NASA, USRA, Google, Temporal Defense Systems

Tab. 5.1: Systémy D-Wave (zdroj:[25], upravené)

Počítače od D-Wave sú často kritizované. Skupina vedcov porovnávala výpočtovú silu klasických a kvantových zariadení od spoločnosti D-Wave, pri čom dospeli

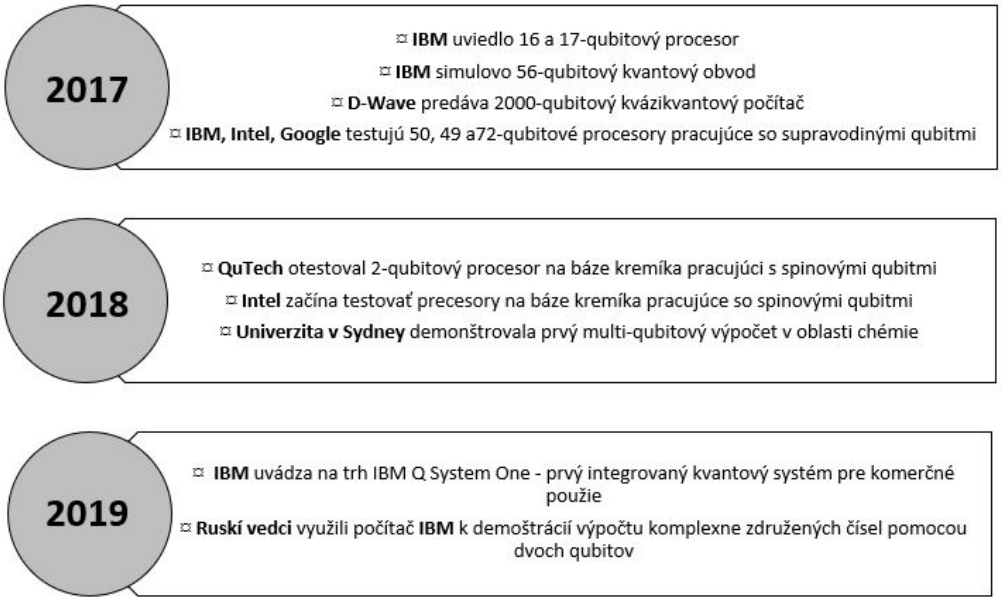
k záveru, že nenašli žiadny dôkaz o kvantovom zrýchlení pre celú množinu testovacích dát. Zároveň však dodávajú, že nevylučujú možnosť zrýchlenia pri riešení iných problémov. [26]. IBM vo svojich článkoch obhajovala fakt, že sa nejedná o kvantový počítač, pretože podľa ich názoru zvyšovanie počtu qubitov nevedie k zvyšovaniu výpočtovej sily — je nutné zaistiť previazanosť qubitov a tiež malú chybovosť, čo počítač od spoločnosti D-Wave nesplňuje[8]. Situáciu reprezentuje obrázok 5.1.



Obr. 5.1: Chybovosť vs. počet qubitov (zdroj:[19], upravené)

5.4 Aktuálny vývoj

Aktuálny vývoj v oblasti kvantových počítačov je zhrnutý na nasledujúcom obrázku. IBM a Google momentálne pracujú na procesoroch využívajúcich Josephsonov efekt. Intel začal postupne testovať procesory na báze kremíka pracujúce so spinovými qubitami.



Obr. 5.2: Aktuálny vývoj v oblasti kvantových počítačov

6 Kryptoanalytické algoritmy

Bezpečnosť klasických kryptografických algoritmov je často založená na časovej obtiažnosti riešenia matematických problémov. Medzi najčastejšie využívané matematické problémy patria: celočíselný faktorizačný problém, problém diskrétneho logaritmu a diskrétny logaritmus prvku eliptickej krivky. Všetky tieto problémy sú riešiteľné pomocou Shorovho algoritmu [27]. Druhým významným algoritmom je Groverov algoritmus, ktorý umožňuje kvadratické zrýchlenie útoku hrubou silou. Jeho implementácia na kvantovom počítači tak vynúti zdvojnásobenie dĺžky kľúča pri symetrických algoritmoch.

Algoritmus	Dĺžka kľúča	Aktuálna efektívna dĺžka kľúča (podľa NIST SP 800-57)	Post-kvantová efektívna dĺžka kľúča
RSA-1024	1024 b	80 b	0 b
RSA-2048	2048 b	112 b	0 b
ECC-256	256 b	128 b	0 b
AES-128	128 b	128 b	64 b
AES-256	256 b	256 b	128 b

Tab. 6.1: Efektívna dĺžka kľúča vybraných algoritmov

6.1 Shorov algoritmus

Už v roku 1994 predstavil Peter W. Shor postup pre kvantový počítač, ktorý efektívne rieši faktorizačný problém pomocou kvantového paralelizmu. Algoritmus nehľadá prvočíselné súčinitele priamo, ale faktorizáciu čísel prevádza na problém hľadania periodickej funkcie. Algoritmus funguje v polynomiálnom čase ($\log n$, kde n je veľkosť vstupu) a poskytuje exponenciálne zrýchlenie oproti súčasným algoritmom [13].

Riešenie faktorizačného problému pomocou Shorovho algoritmu by sa dalo zhrnúť do nasledujúcich bodov:

1) Majme N, ktoré vzniklo ako násobok prvočísel p a q.

2) Zvoľme $a \in \mathbb{Z}_N$ také, že $\gcd(a, N) = 1$

3) Predpokladajme funkciu: $f(x) = a^x \mod N$.

4) Nájsť periódu tejto funkcie znamená, nájsť ω také, že $f(x + \omega) = f(x)$. Z toho vyplýva, že ω je násobkom stupňa prvku $a \mod N$, teda:

$$f(x + \omega) = f(x) \iff a^x \mod N. \tag{6.1.1}$$

Prevod faktorizačného problému na problém hľadania periódy bol známy skôr, ako Shor prišiel s myšlienkou svojho algoritmu. Jeho prínos v tejto oblasti spočíval v tom, že stanovil spôsob ako využiť kvantový počítač pri hľadaní periódy. Kvantový počítač je schopný počítať modulárnu exponenciálnu funkciu pre všetky možné hodnoty x a nakoniec sa pokúsiť vybrať periódu r. Shorov algoritmus na tento výpočet využíva kvantovú Fourierovu transformáciu definovanú ako:

$$|x\rangle \xrightarrow{\text{QFT}} |y\rangle \, 1/2^{n/2} \sum_{y=0}^{2^n-1} e^{i2\pi xy/2^n} \tag{6.1.2}$$

,

kde xy je počítané bežným celočíselným násobením. Táto operácia, rovnako ako bežná Fourierova transformácia, sústredí väčšinu amplitúd na hodnoty y blízke požadovanej perióde r. Meranie finálneho stavu prinesie s veľkou pravdepodobnosťou požadovanú periódu r.

Posledná fáza algoritmu je založená na predošlých matematických poznatkoch (Čínska veta o zbytkoch, Malá Fermatova veta) a to nasledujúco. Ak je r nepárne a ak $a^{r/2} \mod N \neq N-1$, potom aspoň jedno číslo z $\gcd(N, a^{r/2} \pm 1)$ je netriviálny faktor N. Ak r nemá požadované vlastnosti (čo je však málo pravdepodobné) zvolíme iné a. Tým sme našli požadovaný faktor čísla N [1].

Podstata Shorovho algoritmu spočíva v deštruktívnej interfencii. Každý stav v superpozícii ovplyvňuje ostatné stavy zodpovedajúce možnej perióde funkcie. Stavy nevedúce k nájdeniu vyhovujúcej periódy majú opačné amplitúdy, čím sa deštruktívnou interferenciou vyrušia. Stavy vyhovujúcej periódy majú amplitúdy rovnakého smeru, preto s vysokou pravdepodobnosťou nájdeme správnu periódu a tým aj prevedieme faktorizáciu daného čísla [28].

6.1.1 Dopad Shorovho algoritmu na bezpečnosť

Implementácia Shorovho algoritmu na kvantovom počítači bude mať vážny dopad na dnes používané kryptosystémy — RSA, DSA, Diffie-Hellman, ECDH (Diffie-Hellman založený na eliptických krivkách) či ECDSA (DSA založený na eliptických krivkách). Vytvorenie kvantového počítača bude znamenať koniec možnosti používania týchto systémov. Práve preto sú už dnes vyvíjané iné systémy, ktoré sú odolné voči útokom realizovaných na kvantových počítačoch (viac v kapitole 7).

Faktorizačný problém

Faktorizačný problém je označenie pre celočíselný rozklad zloženého čísla na násobky menších celý čísel. Momentálne nie je známy efektívny nekvantový algoritmus pre faktorizáciu (nevyriešeným problémom ostáva, či takýto algoritmus vôbec

existuje). Shorov algoritmus umožňuje riešiť problém prvočíselnej faktorizácie v čase $O(\log n)$, kde n je počet bitov faktorizovaného čísla. To znamená, že použitím tohto algoritmu je možné prelomiť RSA kryptosystém.

Problém diskrétneho logaritmu

Diskrétnym logaritmom sa označuje s v rovnici $b^s = a$, čísla a so základňou b, inak napísané $s = \log_b a$. Vzhľadom k tomu, že problém diskrétneho logaritmu je možné previesť na faktorizačný problém (pre viac detailov odkazujeme čitateľa na [29]), je ho možné vyriešiť v polynomiálnom čase. Shorov algoritmus umožňuje prelomenie DSA, a tiež algoritmu Diffie-Hellman pre výmenu kľúčov.

Problém nájdenia diskrétneho logaritmu prvku eliptickej krivky

Shor rovnako dokázal, že jeho algoritmom je možné riešiť aj diskrétny algoritmus na eliptickej krivke, čo znamená, že je pomocou tohto algoritmu možné prelomiť ECDH — Diffie-Hellman založený na eliptických krivkách, ECDSA - DSA založený na eliptických krivkách [13].

6.2 Groverov algoritmus

Groverov algoritmus predstavuje postup pre kvantový počítač, ktorý umožňuje nájsť konkrétny vstup pre funkciu. Algoritmus zoberie funkciu, a skrz zoznam všetkých možných vstupov pre túto funkciu vyhľadá ten, pre ktorý s vysokou pravdepodobnosťou vráti funkcia hodnotu true. Pokiaľ má funkcia N možných vstupov, algoritmus vráti výsledok v $O(\sqrt{N})$ čase pri čom potrebuje $O(\log N)$ pamäte. Oproti klasickému výpočtu poskytuje kvadratické zrýchlenie, čo znamená, že pri útoku hrubou silou je možné nájsť 128-bitov dlhý symetrický kľúč v približne v 2^{64} iteráciach. V dôsledku toho je možné povedať, že ak chceme zachovať symetrickú kryptografiu, je nutné dĺžku kľúča minimálne zdvojnásobiť [30].

Vstup Groverovho algoritmu tvorí operácia (často označovaná ako kvatové orákulum), ktorej funkcia a zoznam prvkov, s ktorými bude algoritmus pracovať. Orákulum je pri konvenčných počítačoch definované ako:

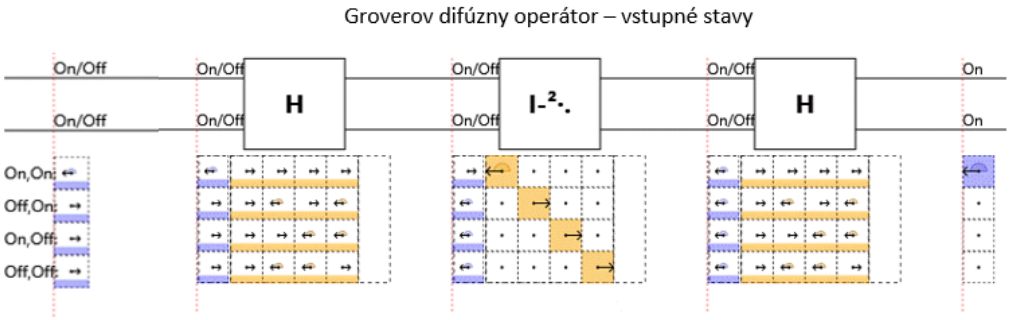
$$f(x) = \begin{cases} 1, & \text{pre } x = x^* \\ 0, & \text{pre } x \neq x^*, \end{cases} \tag{6.2.1}$$

kde x^* predstavuje hľadaný prvok. Orákulum v kvantovom počítaní predstavuje matica U_f, ktorá je pre pri aplikácií na stav $|x\rangle$ definovaná ako:

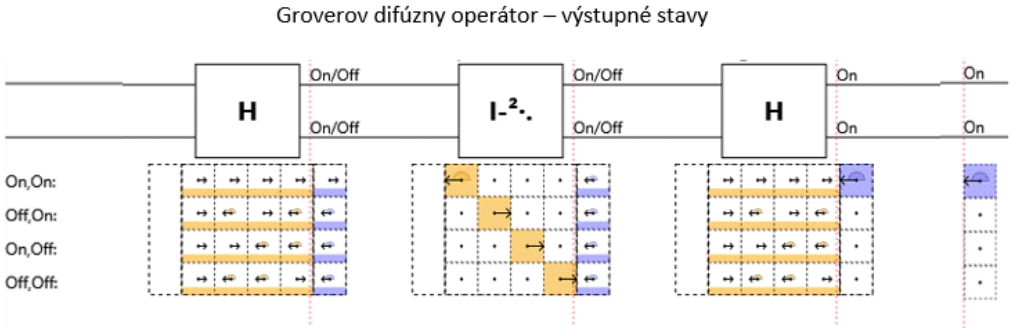
$$U_f(x)\,|x\rangle = (-1)^{f(x)}\,|x\rangle\,. \tag{6.2.2}$$

Orákulum aplikované na všetky prvky (okrem hľadaného prvku) bude vracať pôvodný prvok. Orákulum aplikované na hľadaný prvok vracia výstup $-|x\rangle$. Pravdepodobnosť výberu jednotlivých stavov zostane prechodom cez orákulum rovnaká [30].

Jadrom celého algoritmu je operácia označovaná ako „Groverov difúzny operátor“, ktorá počíta priemer všetkých amplitúd a následne invertuje všetky tieto amplitúdy, pričom najväčšia hodnota amplitúdy patrí hľadanému výsledku. Groverov difúzny operátor je zložený z operácií Hadamard a operácie, ktorá invertuje fázu prvého stavu. Na obrázku č. 6.1 je zobrazené ako vyzerajú jednotlivé stavy pred vstupom do operácií, a na obrázku č. 6.2 je znázornený výstup pre tieto stavy.



Obr. 6.1: Groverov difúzny operátor (vstupné stavy)



Obr. 6.2: Groverov difúzny operátor (výstupné stavy)

Algoritmus teda funguje nasledovne: naprv orákulum spôsobí, že amplitúda stavu, ktorý je výsledkom je iná oproti ostatným amplitúdam a následne Groverov difúzny operátor zistí, ktorá je odlišná. Tento postup sa opakuje, kým nie je pravdepodobnosť dosiahnutia výsledku dostatočne vysoká [30].

6.2.1 Dopad Groverovho algoritmu na bezpečnosť

Groverov algoritmus je významný v oblasti symetrických kryptosystémov. Zatiaľ nie je známky nekvantový efektívny algoritmus umožňujúci priame útoky na symetrické kryptosystémy. Groverov algoritmus ale umožňuje kvadratické zrýchlenie útoku hrubou silou – v dôsledku toho je možné povedať, že konštrukcia kvantového počítača vynúti zdvojnásobenie dĺžky symetrického kľúča.

7 Post-kvantová kryptografia

Post-kvantová kryptografia je označenie pre taký druh kryptografie, ktorý je odolný voči útokom realizovaných prostredníctvom bežných ale i kvantových počítačov [31]. Momentálne existujú štyri základne smery, ktorými sa uberá výskum:

- **Kryptosystémy využívajúce hashe** – konštrukcia kryptosystémov je založená na bezpečnosti hashovacích funkcií. Do tejto kategórie patrí XMSS (exTended Merkle Signature Scheme) alebo SPHINCS.
- **Kryptosystémy využívajúce teóriu kódovania** – bezpečnosť je založená v obtiažnosti dekódovania neznámeho kódu na opravu chýb. Patria sem kryptosystémy používajúce binárne Goppové kódy (cryptosystems based on Goppa codes) alebo klasifikačné kódy (Rank-metric codes).
- **Kryptosystémy využívajúce polynomiálne rovnice** – bezpečnosť vychádza z ťažkosti riešenia systému polynomiálnych rovníc, u ktorých je dokázané že sú buď NP-ťažké alebo NP-úplné. Polynomiálne rovnice vyžíva napríklad podpisová schéma Rainbow alebo schéma Oil and Vinegar.
- **Kryptosystémy využívajúce mriežky** – tento typ kryptosystémov využíva mriežky dvomi možnými spôsobmi: buď v samotnej konštrukcii algoritmu, alebo pri dôkaze ich bezpečnosti. Medzi tieto kryptosystémy môžeme zaradiť NTRU pre šifrovanie a podpisovanie alebo schému BLISS (Bimodal Lattice Signature Scheme) určenú na podpisovanie [32].

7.1 Kryptografia založená na hashoch

Kryptografia založená na hashoch je označenie pre postkvantovú kryptografiu, ktorej bezpečnosť závisí na hashovacích funkciách. Hashovaciu funkciu môžeme označiť za kryptograficky bezpečnú, ak je bezkolízna (collision resistant), odolná voči nájdeniu vzoru (preimage resistant) a odolná voči nájdeniu druhého vzoru (second preimage resistance)[33]. Kryptografia založená na hashoch je momentálne cielená na využitie v oblasti digitálnych podpisov, kde podpisové schémy môžu kombinovať napríklad Merklovu podpisovú schému a jednorázové podpisy[34].

7.1.1 Jednorázové podpisy

Jednorázovým podpisom, ako už vyplýva z názvu, môžeme rozumieť podpis, ktorý bude po vygenerovaní použitý iba raz tj. je možné ho využiť k bezpečnému podpisu jedinej správy. V opačnom prípade, ak bude opakovane použitý rovnaký súkromný kľúč, je znižovaná bezpečnosť podpisu. Tento systém podpisovania bol po prvý

krát predstavený v roku 1979 Leslie Lamportom, kedy vznikla Lamportova schéma pre jednorázové podpisy [35].

Špecifickým problémom jednorázových podpisov je veľkosť kľúčov a podpisov, ktoré sú generované. Prvú možnosť zmenšenia veľkosti kľúča a podpisu priniesla Merklova schéma, ktorá znižuje veľkosť verejného kľúča o polovicu a tiež znižuje veľkosť (niektorých) podpisov. Ďalšie vylepšenie priniesol Robert Winternitz, ktorému sa podarilo znížiť veľkosť verejného kľúča a podpisu na štvrtinu až osminu, čo však vyústilo k zvýšeniu času potrebného na podpisovanie a na verifikáciu podpisu [36].

Lamportova schéma

K demonštrácií použitia Lamportovej schémy bude využitý príklad. Alica chce podpísať 256-bitovú správu, k čomu potrebuje najprv vygenerovať súkromný a verejný kľúč.

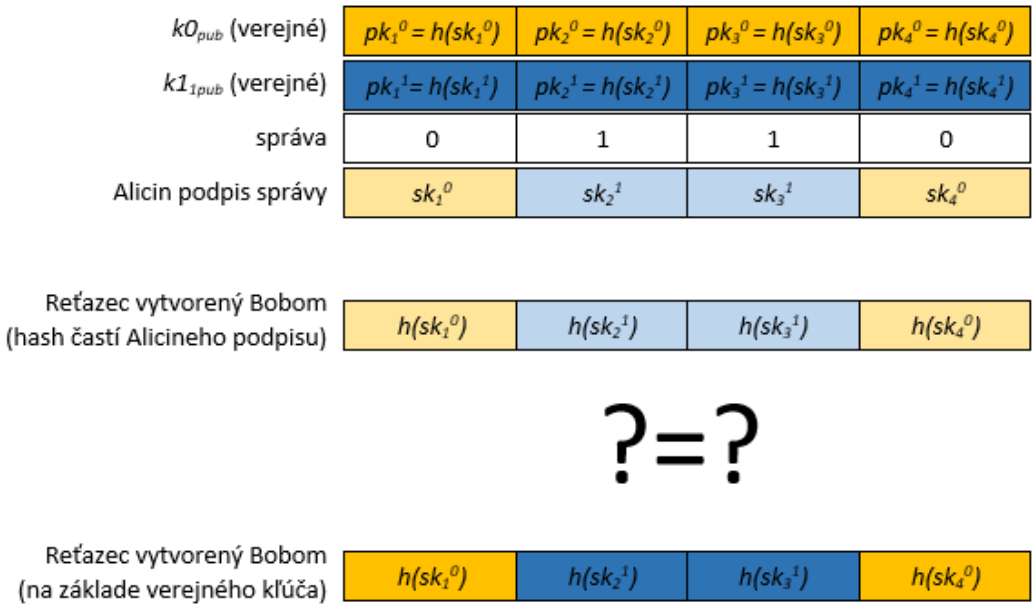
Súkromný kľúč Alica vytvorí tak, že vygeneruje dva zoznamy, pričom každý z nich bude obsahovať 256 náhodných reťazcov. Každý z reťazcov bude dlhý 256b tj. jeden zoznam bude dlhý 65536 bitov. Prvý reťazec označíme $k0_{sk} = sk_1^0, sk_2^0, ...sk_k^0$, druhý reťazec: $k1_{sk} = sk_1^1, sk_2^1, ...sk_k^1$.

Obr. 7.1: Lampertova schéma pre 4-bitovú správu a 1024-bitový kľúč

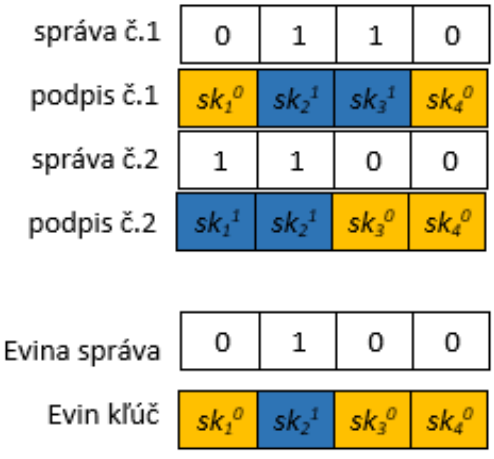
Verejný kľúč vygeneruje Alica pomocou súkromného kľúča tak, že každý reťazec samostatne zahashuje známou funkciou (napr. SHA-256), čím vzniknú dva zoznamy $k0_{pub} = h(pub_1^0), h(pub_2^0), ...h(pub_k^0), k1_{pub} = h(pub_1^1), h(pub_2^1), ...h(pub_k^1)$, ktoré vytvoria verejný kľúč.

Podpisovanie je zobrazené na obrázku 7.1. Správu, ktorú chce Alica podpísať vyjadrí v binárnej podobe. Potom podpisovanie funguje nasledujúco: Alica postupne prechádza správou, a na základe hodnoty bitu vyberie príslušnú časť súkromného kľúča. Teda napríklad ak prvý bit správy bude 0, Alica vyberie zo zoznamu $k0_{sk}$ časť

sk_1^0, ak by bit nadobúdal hodnotu 1, Alica by vybrala zo zoznamu $k1_{sk}$ časť sk_1^1. Je potrebné si však uvedomiť, že každá časť kľúča na obrázku reprezentuje jeden 256-bitový reťazec [36].



Obr. 7.2: Lampertova schéma — overenie správnosti Aliciného podpisu



Obr. 7.3: Lampertova schéma — možnosť útoku pri použití rovnakého kľúča dvakrát

Pri **overení podpisu** Bob po častiach zahashuje Alicin podpis. V prípade, že kľúč nebol cestou útočníkom pozmenený, bude sa vypočítaný hash zhodovať s odpovedajúcimi časťami verejného kľúča Alice. Spôsob overenia ilustruje obrázok 7.2.

Ak by Alica nedodržala pravidlo, že jedným kľúčom môže podpísať jedinú správu, mohla by sa Eva vydávať za Alicu. Eva by na základe rekonštrukcie dvoch podpisov vypočítala Alicin podpis pre ďalšiu správu (obrázok č. 7.3) [36].

Merklova podpisová schéma

Problém množstva kľúčov u jednorázových podpisov rieši Merklova podpisová schéma, kde je jeden verejný kľúč používaný k podpisovaniu viacerých správ (konkrétne k 2^n správ, kde n je počet listov použitého stromu). Nevýhodnou tejto schémy je, že veľkosť kľúča rastie lineárne s počtom poslaných správ [37].

Výstupná dĺžka hashu	128b	160b	224b	256b	384b	512b
Bitová bezpečnosť (klasická krypto.)	63	79	111	127	191	255
Bitová bezpečnosť (post-kvantová krypto.)	0	0	73	84	127	169

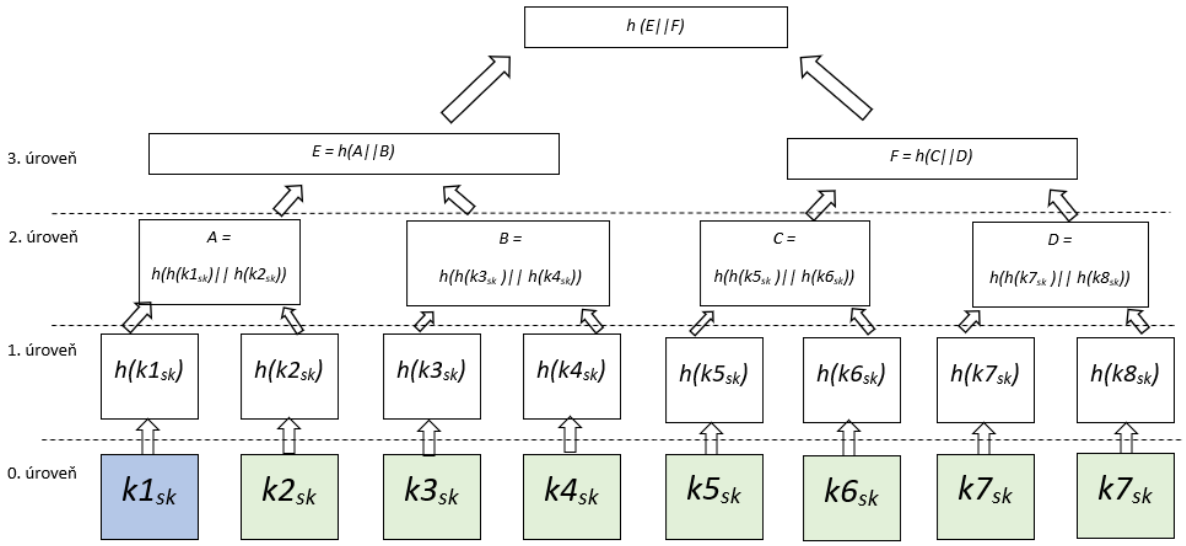
Tab. 7.1: Bezpečnostná úroveň Merklovej podpisovej schémy pri využití Lampertovej schémy (zdroj: [27, str. 98], upravené)

V tomto prípade musí Alica vygenerovať n párov kľúčov pomocou Lamportovej schémy. Kľúče sa uložia do stromovej štruktúry, a to tak, že vytvoria listy stromu. Ostatné uzly v strome sa vypočítajú, až kým neprídeme ku koreňu stromu, ktorý tvorí hlavný kľúč.

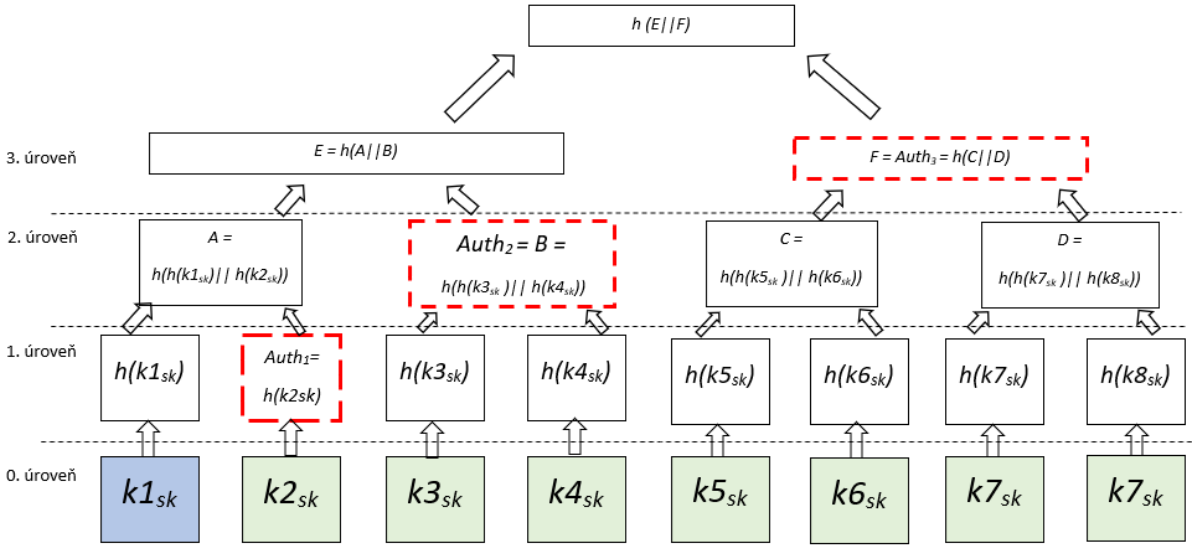
Pri počítaní hodnoty uzlov v strome postupujeme od listov, kedy zahashujeme ich hodnotu, čím vytvoríme prvú úroveň stromu. Druhú úroveň vytvoríme tak, že zreťazíme hodnoty oboch potomkov uzlu a tie následne zahashujeme. Obdobne postupujeme až ku koreňu, ktorý je publikovaný ako verejný kľúč Alice. Proces je zobrazený na obrázku 7.4.

Alica pri podpisovaní vyberie jeden z doposiaľ nepoužitých listov (napr. k_{sk}^1) , pomocou ktorého podpíše správu. Vytvorí tak jednorázový podpis sig^*. K tomu, aby bolo možné overiť, že verejný kľúč bol vypočítaný zo zvoleného listu, bude podpis správy ďalej obsahovať hodnoty vybraných listov $auth_1, .., auth_{n-1}$ — tých, ktorí sú súrodenci rodičovských uzlov vybraného listu (viď obr. 7.5). Dostávame tak podpis správy $sig = sig^*, k_{sk}^1, auth_1, .., auth_{n-1}$, kde n je počet úrovní.

Zo znalosti podpisu a verejného kľúča Alice je Bob schopný overiť, či podpis správy patrí Alici.



Obr. 7.4: Vytvorenie uzlov v strome



Obr. 7.5: Tvorba podpisu

7.2 Kryptografia založená na teórii kódovania

Kryptografia založená na teórií kódovania bola predstavená v rokou 1978, kedy McEliece publikoval svoj kryptosystém. Šifrovanie pomocou tohoto kryptosystému je veľmi rýchle, pretože sa jedná o jedinú operáciu násobenia matice s vektorom. Najväčšou nevýhodou tohto kryptosystému je extrémna veľkosť kľúčov (pre bežné

použitie 524 kb verejný kľúč, 300 kb súkromný kľúč), ktorá je potrebná na zabezpečenie neprelomiteľnosti. Tento fakt spôsobuje to, že v praxi je tento algoritmus využívaný len zriedka. McEliecov kryptosystém je založený na binárnych Goppa kódoch a jeho bezpečnosť spočíva v probléme dekódovania neznámeho lineárneho kódu, čo je NP-ťažký problém [38].

Goppa kódy sa radia medzi účinné kódy pre opravu chýb pri prenose správy medzi prijímačom a vysielačom. Na zabezpečovaciu schému ich prerobíme tým, že kódovacie a dekódovacie funkcie budú tajné. Oproti RSA je algoritmus rýchlejší pri šifrovaní aj dešifrovaní [39].

7.2.1 Kryptosystém McEliece

Pri generovaní kľúčov Alica postupuje tak, že si vyberie lineárny kód so známym algoritmom pre dekódovanie. Lineárny kód bude mať parametre (n, k, z), kde k, n značí rozmery generujúcej matice G a z je počet chýb, ktorý je schopný zvolený kód opraviť. Následne Alica vygeneruje dve náhodné matice – S (regulárna matica s rozmermi $k \times k$) a P (permutačná matica s rozmermi $n \times n$). Z matíc Alica vypočíta $G^* = SGP$. Maticu G^* Alica zverejní ako verejný kľúč s parametrami (n, k, z). Súkromný kľúč tvoria matice (G, S, P) [38].

Alica šifruje tak, že najprv vygeneruje náhodný chybový vektor x s Hammingovou váhou z^2. Správu m o dĺžke k bitov, zašifrujeme nasledovne: $c = mG^* + x$.

Bob obdrží zašifrovanú správu c o dĺžke n bitov. Vypočíta vektor $c^* = cP^{-1}$, ktorý dekóduje zvoleným kódom na vektor m^*. Pôvodnú správu Bob vypočíta ako $m = m^*S^{-1}$.

7.3 Kryptografia založená na mriežkach

Bezpečnosť kryptografie založenej na mriežkach vychádza z problémov, ktoré sú s nimi spojené – napr. SVP (problém hľadania najkratšieho vektoru báze) či CPV (problém hľadania najbližšieho bodu mriežky). Mriežkou rozumieme množinu bodov vn-rozmernom priestore, ktorá má pravidelnú štruktúru. Výhodou tohto prístupu je, že vytváranie kľúčov založených na mriežkach je relatívne jednoduché, efektívne a paralelizovateľné [40].

7.3.1 NTRU

NTRU je kryptosystém, ktorý je rozdelený na dve časti NTRUEncrypt (šifrovanie), NTRUSing (podpisovanie). Jeho bezpečnosť je závislá na SVP probléme.

NTRU kryptosystém využíva teleso, pozostávajúce z polynómov stupňa nanajvýš $N-1$. Systém má viacero parametrov, pričom pre potreby tejto práce budeme označovať:

N — všetky polynómy v telese musia byť stupňa nanajvýš $N-1$, q — veľký modulus: koeficienty polynómov budú redukované $\mod q$, p — malý modulus: koeficienty polynómov budú redukované $\mod q$ pri konečnej fáze dešifrovania.

Pokiaľ chceme zachovať bezpečnosť algoritmu, q a p musia byť zvolené dostatočne veľké (viď. tab. č: 7.2) a nesúdeliteľné.

	N	q	p
Stredná bezpečnosť ($\approx$ RSA512)	167	128	3
Štandardná bezpečnosť	251	128	3
Vyššia bezpečnosť	347	128	3
Najvyššia bezpečnosť ($\approx$ RSA2048)	503	256	3

Tab. 7.2: Bezpečnosť NTRU na základe zvolených parametrov (zdroj: <`https://assets.onboardsecurity.com/static/downloads/NTRU/resources/NTRU-PKCS-Tutorial.pdf`>)

Pri **generovaní kľúčov** Bob náhodne vyberie dva tajné polynómy f a g, patriace do telesa R. Potom vypočíta inverzný polynóm f_q k f ako $f * f_q = 1(\mod q)$ a inverzný polynóm f_p k f ako $f * f_p = 1(\mod p)$. Ak inverzný polynóm neexistuje, zvolí Bob iný polynóm f. Ďalej Bob vypočíta verejný kľúč $h = pf_p * g(\mod q)$.

Pri **šifrovaní** Alica prevedie správu m do tvaru polynómu, ktorého všetky koeficienty sa nachádzajú v telese $(\mod p)$. Ďalej vygeneruje polynóm r (má podobnú funkciu ako náhodná hodnota pri algoritme ElGamal).

Z náhodného polynómu r a verejného kľúča Boba Alica vytvorí šifrovanú správu $e = r * h + m(\mod q)$.

Pri **dešifrovaní** Bob vypočíta polynóm $a = f * e(\mod q)$, pri čom si koeficienty a ležia medzi $-q/2$ a $q/2$. Potom vypočíta $b = a(\mod p)$ a nakoniec vypočíta $c = f_p * b(\mod p)$. Ak správa m nebola cestou zmenená, je rovná c [40].

Príklad:

Generovanie kľúčov

Bob vyberie parametre systému ako $N = 11, q = 32, p = 3$. d_f koeficientov polynómu f bude rovných 1, $d_f - 1$ koeficientov bude rovných -1, zvyšok bude rovný 0. d_g koeficientov polynómu g bude rovných 1, d_g koeficientov bude rovných -1, zvyšok bude rovný 0. Pre potreby výpočtu bude ďalej počítané s $d_f = 4$ a $d_g = 3$. Bob zvolí polynóm f stupňa $N - 1 = 10$, ktorý bude obsahovať $d_f = 4$ koeficientov s hodnotou

1, a $d_f - 1 = 3$ koeficientov s hodnotou -1 a polynóm g stupňa $N - 1 = 10$ s $d_g = 3$ koeficientami s hodnotou 1 a s $d_g = 3$ koeficientami s hodnotou -1.
Napríklad:
$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^10$,
$g = -1 + x^2 + x^3 + x^5 - x^8 - x^10$.
Ďalej spočíta inverzný polynóm
$f_p = 1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + 2x^9$
a $f_q = 5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^5 + 16x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10}$.
A nakoniec spočíta verejný kľúč
$h = pf_p * g(\mod q) =$
$= 2 + 25x + 25x^2 + 20x^3 + 12x^4 + 24x^5 + 15x^6 + 19x^7 + 12x^8 + 19x^9 + 16x^10(\mod 32)$.

Šifrovanie
Polynóm r má byť malý, preto definuje d_r. Polynóm r má d_r koeficientov rovných 1, a d_r koeficientov roných -1, zvyšok je rovný 0. Pre výpočet zvolíme d_r=3.
Alica chce poslať správu $m = -1 + x^3 - x^4 - x^8 + x^9 + x^10$,
zvolí $r = -1 + x^2 + x^3 + x^4 - x^5 - x^7$.
Zašifrovaná správa je potom
$e = r * h + m(\mod q) =$
$= 14 + 11x + 26x^2 + 24x^3 + 14x^4 + 16x^5 + 30x^6 + 7x^7 + 25x^8 + 6x^9 + 19x^{10}$.

Dešifrovanie
Bob dešifruje správu ako
$a = f * e(\mod q) =$
$= 3 - 7x - 10x^2 - 11x^3 + 10x^4 + 7x^5 + 6x^6 + 7x^7 + 5x^8 - 3x^9 - 7x^10$,
ďalej vypočíta $b = a(\mod p) = -x - x^2 + x^3 + x^4 + x^5 + x^7 - x^8 - x^{10}$
a nakoniec využije svoj súkromný kľúč
$c = f_p * b(\mod p) = -1 + x^3 - x^4 - x^8 + x^9 + x^{10}$.

7.4 Kryptografia založená na polynomiálnych rovniciach

Kryptografia založená na polynomiálnych rovniciach je pojem označujúci kryptosystémy založené na mnohorozmerných polynómoch nad konečným poľom F. Bezpečnosť algoritmov je založená na probléme riešenia systémov polynomiálnych rovníc, čo je NP-ťažký alebo NP-úplný problém.

7.4.1 QUAD

Prúdová šifra QUAD bola prestavená v roku 2016 a jej bezpečnosť je založená na MQ probléme. MQ problém spočíva v obtiažnosti nájdenia riešenia sústavy kvadratických rovníc o viacero premenných nad konečnými telesami. Autori odporúčajú pri využití tejto šifry používať 80-bitové kľúče, 80-bitový inicializačný vektor a vnútorný stav systému dlhý 160 bitov [41].

Generovanie keystreamu

Verejné parametre systému bude predstavovať trojica S, S_1, S_2. Najprv náhodne vygenerujeme kn polynómov druhého stupňa o n premenných nad konečným telesom $GF(q)$ (označíme ako $S = (P_1, \ldots, P_{kn})$), skrátene je možné označovať ako (k, n, q). Ďalej označíme ako S_0 a S_1 dva náhodne polynomiálne systémy tvorené n polynómami a n premennými nad telesom $GF(q)$. Stav vnútorného registru $x = x_1, \ldots, x_n$ tvoria n-tice hodnôt $GF(q)$.

Samotné generovanie keystreamu spočíva v opakovaní troch krokov popísaných nižšie, pričom je v každej iterácii generovaných $(k-1)n$ hodnôt. Generovanie keystreamu začneme prvým krokom, ktorý spočíva vo vypočítaní kn hodnôt systému $S(x) = (P_1(x), \ldots, P_{kn}(x))$, kde x je aktuálny vnútorný stav generátora. V druhom kroku sa reťazec $S(x)$ následne rozdelí na dve časti – jedna časť tvorí vstup ďalšej iterácie (n prvých členov), druhá časť je výstupom generátora ($(k-1)n$ členov). Tretí krok spočíva v aktualizácii vnútorného stavu x s prvými n hodnotami reťazca $S(x)$. Počiatočná hodnota reťazca $S(x)$ môže byť zvolená náhodne, ale šifra QUAD má mechanizmus, ako túto hodnotu počítať z inicializačného vektora a zo zadaného kľúča [41].

Šifrovanie a dešifrovanie

Šifrovanie prebieha tak, že sa otvorený text sčíta s keystreamom v telese $GF(q)$. Pri dešifrovaní naopak prebieha odčítanie keystremu od zašifrovanej správy v telese $GF(q)$.

8 Výuková aplikácia

V rámci tejto práce bola vytvorená webová stránka slúžiaca pre výukové účely (stránka je dostupná z: `https://sites.google.com/view/kvantova-kryptografia`). Stránka je rozdelená do štyroch samostatných častí:

- základy kvantového počítania a teórie kvantovej informácie,
- kvantové logické funkcie,
- kryptoanalytické algoritmy,
- a kvantovo bezpečná kryptografia.

V časti *Základy kvantového počítania a teórie kvantovej informácie* je čitateľ zoznámený so základmi kvantovej fyziky nevyhnutnej pre pochopenie ďalšieho textu a laboratórnych úloh. V časti *Kvantové logické funkcie* je pozornosť venovaná jednotlivým logickým operáciám (Pauliho X-operácia, Pauliho Y-operácia, Pauliho Z-operácia, operácia Hadamard). Teoretický výklad je doplnený animáciami, ktoré ilustrujú aplikáciu jednotlivých operácií na qubit. Pasáž *Kryptoanalytické algoritmy* sa zaoberá vysvetleniu Shorovho a Groverovho algoritmu. Nedeliteľnou súčasťou sú dve laboratórne úlohy orientované na praktickú aplikáciu kvantových operácií a na vytvorenie Groverovho algoritmu pomocou kvantového simulátoru Quirk (úlohy sú uvedené v kapitole 8.1 a 8.2). Podstránka *Kvantovo bezpečná kryptografia* v krátkosti predstavuje štyri základné smery, ktorými sa post-kvantová kryptografia momentálne uberá a následne sú v tejto časti prezentované jednorázové podpisy (vrátane Merklovej schémy) a prúdová šifra QUAD. Časť je doplnená o animácie ilustrujúce jednotlivé časti algoritmov.

8.1 Laboratórna úloha č.1 – úvod do práce s kvantovým simulátorom

Cieľ úlohy: Cieľom tejto úlohy je zoznámiť študenta so základmi kvantových operácií a to pomocou simulácie kvantového počítača, pričom budú využité základy lineárnej algebry – vektorové a maticové operácie. Po ukončení tejto úlohy by študent mal byť schopný zvládnuť vytvoriť jednoduchý kvantový obvod pomocou simulátoru Quirk.

8.1.1 Kvantové spracovanie informácií

Bit, ako klasická jednotka informácie, môže nadobúdať dva vzájomne sa vylučujúce stavy (0 a 1). Pri kvantovom počítaní sa využíva ako základná jednotka informácie **qubit**. Ten na rozdiel od bitu môže byť tvorený ľubovoľnou lineárnou kombináciou

0 a 1, čo môžeme vyjadriť pomocou vzťahu:

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \ c_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{8.1.1}$$

kde c_1, c_2 sú komplexné čísla, nazývané amplitúdy pravdepodobnosti. **Amplitúda pravdepodobnosti** predstavuje číslo priradené neurčitému stavu (nie je možné priamo merať), ktoré spĺňa podmienku $|c_1|^2 + |c_2|^2 = 1$. Druhú mocninu čísla c_1 je možné interpretovať ako pravdepodobnosť nájdenia $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$ v stave $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Ďalšou vlastnosťou qubitu je jeho **veľkosť** – počíta sa rovnako ako v prípade veľkosti komplexného čísla tj.$\sqrt{{c_1}^2 + {c_2}^2}$ [1, str. 10-15].

Pre skrátený zápis qubitu je možné využiť aj tzv. Diracovu notáciu, kde sa stav $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ zapisuje ako |1>, stav $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ako |0> a všeobecný stav je označovaný $|\psi>$. Rovnako dobre je qubity možné vyjadrovať formou komplexného čísla napr. stav $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ je možné zapísať ako $1 + 0i$.

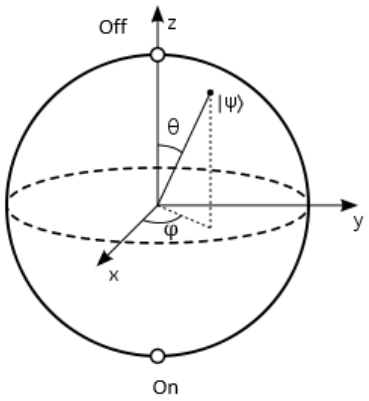
Poznámka: Simulátor Quirk často označuje stav $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ *ako Off a stav* $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ *ako On.*

Flexibilitu jedného qubitu je možné dobre reprezentovať pomocou **Blochovej sféry** (obr. č. 8.1). Tá umožňuje tiež jednoduché ale výkonné zobrazenie správania sa qubitu. Póly sféry reprezentujú stavy Off a On; všeobecné stavy pokrývajú celú plochu sféry. Uhol θ vyjadruje pravdepodobnosť namerania stavu Off – ak sa stav nachádza„bližšie“k severnému pólu je pravdepodobnejšie, že pri meraní všeobecný stav skolabuje do bázového stavu Off. Ak sa stav nachádza priamo na rovníku, existuje pravdepodobnosť 0,5, že pri meraní skolabuje do stavu On a pravdepodbnosť 0,5, že skolabuje do stavu Off. Na druhú stranu, rotácia okolo osy z vyústi do fázového posunu, čo pri meraní žiadnym spôsobom neovplyvní stav, do ktorého qubit skolabuje. Táto rotácia je reprezentovaná zmenou uhlu φ [5].

Najdôležitejším javom, ktorý sprevádza qubity je **superpozícia**. Superpozíciou môžeme zjednodušene nazvať vlastnosť qubitu, kedy sa systém nachádza vo viacerých stavoch, až pokiaľ nebude vykonané meranie. V skutočnosti to znamená, že superpozícia nikdy nebude môcť byť nameraná, pretože ju meranie naruší. Ak uskutočníme meranie v superpozícií, mali by sme dostať výsledok: „qubit sa nachádza v stave Off s pravdepodobnosťou c_1^2 a v stave On s pravdepodobnosťou c_2^2 “. Pri meraní však nastane interferencia, čo výusti do toho, že qubit skolabuje buď do stavu On alebo do stavu Off (Off s pravdepodobnosťou c_1^2, On s pravdepodobnosťou c_2^2) – žiadny stav „medzi “nenameriame [2].

8.1.2 Vytváranie systémov z viacerých qubitov

Reálna sila kvantových počítačov sa prejaví až v prípade systému zloženého z dvoch a viac qubitov, kedy sa začne prejavovať **kvantové previazanie**. Pri previazaní



Obr. 8.1: Blochova sféra

viacerých qubitov v superpozícií sa začnú jednotlivé qubity navzájom ovplyvňovať, čo znamená, že zmeranie jediného qubitu zo systému spôsobí kolaps celého systému. Meranie teda spôsobí to, že všetky qubity opustia superpozíciu a skolabujú do jedného zo stavov On a Off .

Poznámka: Simulátor Quirk vytvára automaticky systém s qubitmi, ktoré sú previazané.

Vytvoriť systém, ktorý pozostáva s viac ako jedného qubitu znamená použiť operáciu tenzorový súčin, čo si zjednodušene môžeme predstaviť ako „inak napísané maticové násobenie“. Na vysvetlenie použijeme všeobecný príklad [5].

$$\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \otimes \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \cdot 4 \\ 1 \cdot 5 \\ 2 \cdot 4 \\ 2 \cdot 5 \\ 3 \cdot 4 \\ 3 \cdot 5 \end{bmatrix}. \tag{8.1.2}$$

V kvantovom počítaní potom pracujeme pri vytváraní viacqubitových systémov

nasledujúco. Napríklad stav |011> vytvoríme ako:

$$\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\cdot 0\cdot 0\\1\cdot 0\cdot 1\\1\cdot 1\cdot 0\\1\cdot 1\cdot 1\\0\cdot 0\cdot 0\\0\cdot 0\cdot 1\\0\cdot 1\cdot 0\\0\cdot 1\cdot 1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix}. \tag{8.1.3}$$

Takýto systém môže naraz vykonávať výpočty s 2^8 stavov, čím sa stáva neporovnateľnejšie výpočtovo výkonnejší ako bežný počítač.

8.1.3 Kvantové operácie

Kvantové operácie prestavujú spôsob ako manipulovať s qubitmi. Operácie musia byť reverzibilné, čo znamená, že sú časovo invertovateľné. Medzi základné kvantové operácie patrí operácia NOT (Pauliho X-operácia), Pauliho Z-operácia a operácia Hadamard.

Pauliho X-operácia

Pauliho X-operácia pracuje s jedným qubitom. Jej funkcia je ekvivalentná použitiu operácie NOT pri klasických počítačoch. V Blochovej sfére predstavuje rotáciu stavu okolo osi x o π radiánov. Matematicky sa operácia uskutoční tak, že sa maticou X vynásobí pôvodný stav [7].

$$X = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}. \tag{8.1.4}$$

Pauliho Z-operácia

Pauliho Z-operácia pracuje s jedným qubitom. Zobrazuje stav |0> =|0>, a |1> =− |1>. Operácia je v Blochovej sfére reprezentovaná rotáciou okolo osi z o π radiánov. Matematicky sa operácia uskutoční tak, že sa maticou Z vynásobí pôvodný stav [7].

$$Z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}. \tag{8.1.5}$$

Obdobnou operáciou je $Z^{1/4}$-operácia ($Z^{-1/4}$-operácia), ktorá pracuje obdobne s tým rozdielom, že rotácia je 45° (−45°).

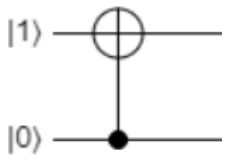
Operácia Hadamard

Operácia Hadamard pracuje s jedným qubitom. Zobrazuje stav $|0> = \frac{|0> + |1>}{\sqrt{2}}$, a $|1> = \frac{|0> - |1>}{\sqrt{2}}$. Operácia spôsobní, že na výstupe systému bude pravdepodobnosť namerania stavu On a Off rovnaká (0,5). Na Blochovej sfére je reprezentovaná dvomi rotáciami – o π radiánov okolo osi z a následne o π radiánov okolo osy y. Matematicky sa operácia uskutoční tak, že sa maticou H vynásobí pôvodný stav [7].

$$H = 1/\sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{8.1.6}$$

Kontrolné bloky

Okrem operácií je možné pri zostavovaní obvodov využiť aj kontrolné bloky – Control a Anti Control. Pri spojení operácie na qubite B s kontrolným blokom Control umiestneným na qubite A, bude operácia na qubite B vykonaná iba v prípade, ak na qubite A bude stav On (pre Anti Control sa kontroluje stav Off). Napríklad obr. č. 8.2 vyjadruje, že Pauliho X-operácia bude vykonaná iba v prípade, ak qubit B bude v stave On (v tomto prípade sa teda operácia realizovať nebude, pretože vstupný stav qubitu B je Off, pričom nezáleží na stave qubitu A).

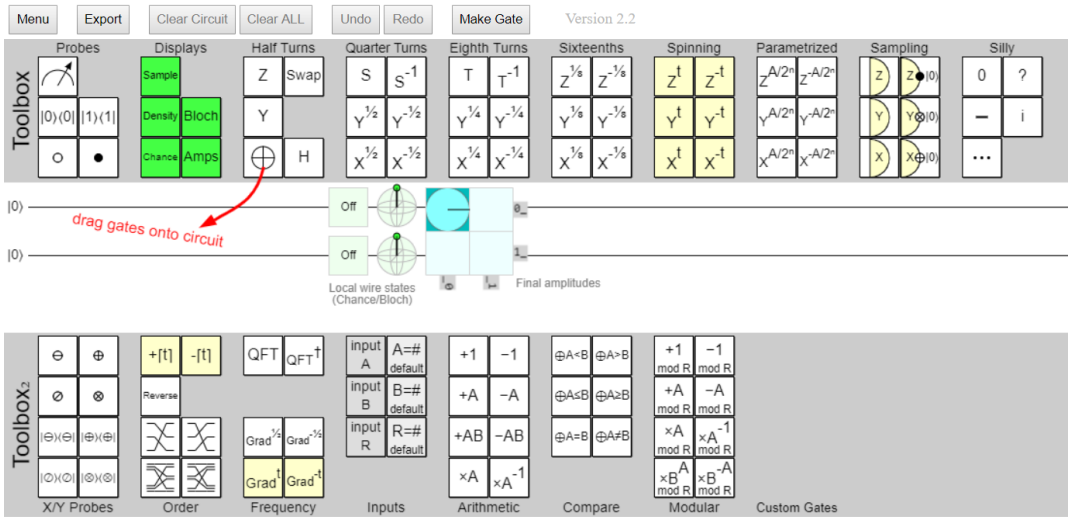


Obr. 8.2: Kontrolný blok

8.1.4 Kvantový simulátor – Quirk

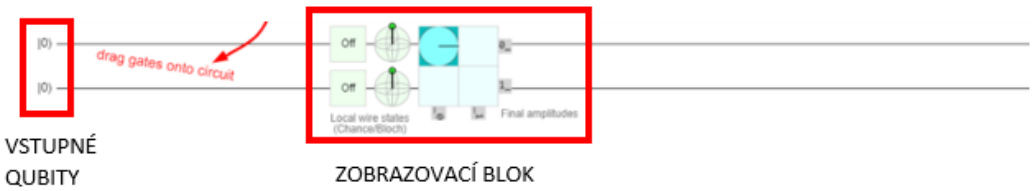
Quirk je kvantový simulátor, ktorý umožňuje vytvárať kvantové obvody. Je dostupný z adresy https://algassert.com/quirk. Po otvorení odkazu sa zobrazí stránka *Welcome to Quirk*, kde je potrebné vybrať možnosť *Edit Circuit*. Po načítaní by sa mala zobraziť úvodná obrazovka (obr. č. 8.3).

Stredná časť obrazovky (obr. č. 8.4), prestavuje aktuálny logický obvod. Na jeho začiatku môžeme vidieť, že obvod má dva vstupné qubity nastavené v stave Off a Off. Horný qubit budeme ďalej označovať ako qubit A, dolný qubit ako B. Ďalej môžeme vidieť „zobrazovací blok“, ktorý na Blochovej sfére reprezentuje výstupné



Obr. 8.3: Úvodné zobrazenie simulátoru Quirk

stavy qubitov. Podržaním kurzoru na jednotlivých sférach je možné vidieť podrobnosti o jednotlivých qubitoch. Za Blochovou sférou nasleduje zobrazenie amplitúdy. Každá štvorcová časť v zobrazení predstavuje jednu amplitúdu. Polomer modrého kruhu reprezentuje veľkosť amplitúdy a uhol čiernej čiary zobrazuje fázu amplitúdy. Výška tmavomodrej výplne je pravdepodobnosť amplitúdy [anglicky mag^2].



Obr. 8.4: Simulátor Quirk – vstupné quibity a zobrazovací blok

8.1.5 Námety na samostatnú prácu

Táto kapitola pozostáva z piatich úloh, pričom každá môže byť vykonaná zvlášť. Po ukončení každej úlohy vráťte simulátor do východzej pozície (tj. na vstupoch A a B je stav Off).

Samostatná úloha č.1

- Simulátor Quirk ponechajte vo východziom stave.

- Pomocou zobrazovacieho bloku zistite, aká je aktuálna pravdepodobnosť namerania stavu On na qubite A.
- Aký uhol zviera qubit A s osou z a s osou x v Blochovej sfére?
- Akú súradnicovú reprezentáciu má qubit A v Blochovej sfére? Odpoveď zapíšte v tvare A $[x, y, z]$.
- Zmeňte počiatočný stav qubitu A na On (kliknutím na vstupný stav qubitu). Zodpovedajte predchádzajúce otázky.

Samostatná úloha č.2

- Vytvorte systém, ktorý bude mať na vstupe A $\begin{bmatrix}0\\1\end{bmatrix}$ a na vstupe B $\begin{bmatrix}1\\0\end{bmatrix}$.
- Na qubit B aplikujte Pauliho-X operáciu. Aký bude výsledný stav systému? Overte pomocou matematického výpočtu.
- X-operáciu zviažte s kontrolnou operáciu na stav A. Čo sa zmenilo? Akým spôsobom funguje práve zostrojený obvod?
- Obvod zmeňte tak, aby Pauliho-X operácia bola prevedená iba v prípade, ak stab qubitu A bude Off.
- Na vstup A nastavte Off. Aký bude výstup systému?

Samostatná úloha č.3

- Zostrojte systém v simulátore Quirk, ktorý bude vykonávať operáciu SWAP. Počiatočné nastavenie systému:
  - Vstupy A a B budú v stave On.
  - Obvod bude vytvárať negáciu qubitu A v prípade, ak na vstupe B bude 1.
  - Následne obvod overí qubit A, a ak bude v stave On, vytvorí negáciu qubitu B.
  - Následne obvod vytvorí negáciu qubitu A, ak bude v qubit B v stave On.
- Zmeňte vstup B na Off. Aký bude výstupný stav quibitov?
- Vyskúšajte rôzne kombinácie vstupov a popíšte správanie tohto systému.

Samostatná úloha č.4

- Uveďte qubit A do superpozície.
- Aký bude výstup tohto systému (určte stavy a ich pravdepodobnosti)?
- Doplňte systém tak, aby pravdepodobnosti všetkých výstupov boli rovné 0,25.

- Za aktuálne vytvorený systém doplňte operácie na qubite A tak, aby bol qubit A negovaný v prípade, ak stav B bude On. Čo sa zmenilo na výstupe? Svoju odpoveď zdôvodnite.
- Aktuálne vytvorený systém upravte tak (bez toho aby ste odstránili všetky bloky), aby na výstupe boli rovnaké stavy ako na vstupe.

Samostatná úloha č.5

- Vstup A nastavte na On.
- Na qubit A aplikujte Z-operáciu. Čo sa zmenilo na Blochovej sfére a čo na amplitúdach výstupného systému?
- Predchádzajúcu odpoveď matematicky dokážte (aplikujte Z-operáciu v maticovej podobe na vstup A).
- Za aktuálne vytvorený systém doplňte operácie na qubite A tak, aby bol qubit A negovaný v prípade, ak stav B bude On. Čo sa zmenilo na výstupe? Svoju odpoveď zdôvodnite.
- Je Z operácia reverzibilná? Svoju odpoveď odôvodnite.

8.2 Laboratórna úloha č.2 – Groverov algoritmus

Cieľ úlohy: Cieľom tejto úlohy je vytvoriť obvod pomocou simulátoru Quirk, ktorý bude realizovať Groverov algoritmus.

8.2.1 Pozadie problému

Groverov algoritmus je postup, ktorý umožňuje vyhľadať prvok s jedinečnou vlastnosťou (ďalej označený ako víťaz) v neusporiadanej databáze o n prvkoch využitím $O(\sqrt{n})$ operácií. Konvenčné počítače by podobnú úlohy boli schopné riešiť pomocou $O(n)$operácií. Tento algoritmus tak umožňuje kvadratické zrýchlenie oproti klasickému optimálnemu algoritmu [30].

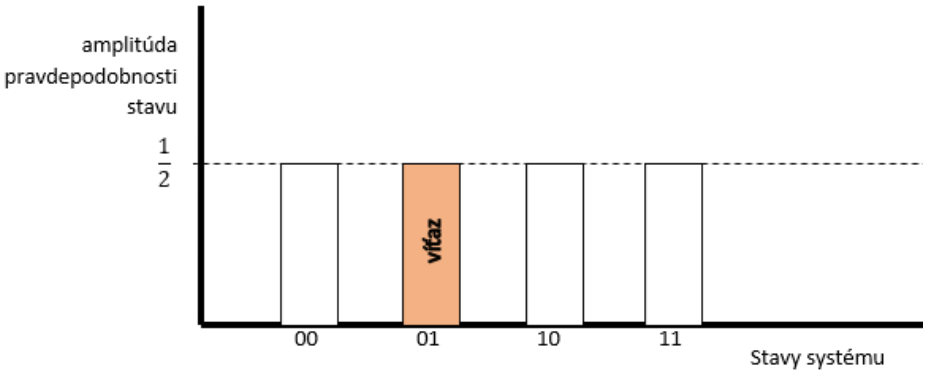
Obr. 8.5: Zoznam s hľadaným víťazom

V kvantovom počítaní budú všetky prvky (vrátane víťaza) nadobúdať binárnu hodnotu. Algoritmus predstavuje spôsob ako zvýšiť pravdepodobnosť nájdenia víťaza, pomocou zosilnenia jeho amplitúdy (tzv. amplitude amplification).

Inicializačná fáza

Prvý krok algoritmu predstavuje uvedenie všetkých možných stavov systému do superpozície, čo pri 1-qubitovom (qubit - kvantový variant konvenčného bitu) systéme znamená že stav $|0>$ prevedieme do stavu $\frac{|0>+|1>}{\sqrt{2}}$ a stav $|1>$ do stavu $\frac{|0>-|1>}{\sqrt{2}}$ [30].

Všetky superponované stavy budú mať rovnakú amplitúdu. Druhá mocnina tejto amplitúdy predstavu pravdepodobnosť pozorovania daného stavu. Uvažujme 2-qubitový systém, ktorý môže nadobúdať stavy |00>,|01>, |10> ,|11>, čo predstavuje obrázok 8.6 .



Obr. 8.6: Inicializácia superponovaných stavov

Pravdepodobnosť jednotlivých stavov bude ¼ (čo vypočítane ako $\left(\frac{1}{2}\right)^2$). Ak v tejto situácií vykonáme náhodný výber bude to znamenať, že každý stav vyberieme s rovnakou pravdepodobnosťou, čo znamená že víťaz bude vybraný s pravdepodobnosťou ¼.

Kvantové orákulum

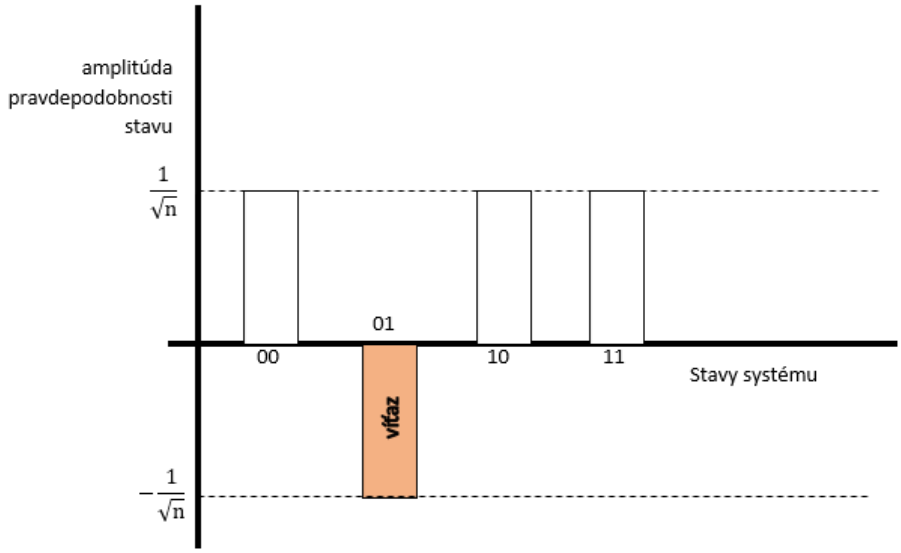
Ďalším krokom Groverovho algoritmu je aplikácia kvantového orákula. Pri konvenčných počítačoch je orákulum definované ako:

$$f(x) = \begin{cases} 1, & \text{pre } x = x^* \\ 0, & \text{pre } x \neq x^*, \end{cases} \tag{8.2.1}$$

kde x^* predstavuje víťaza. Orákulum v kvantovom počítaní predstavuje matica U_f, ktorá je pre pri aplikácií na stav $|x\rangle$ definovaná ako:

$$U_f(x)\,|x\rangle = (-1)^{f(x)}\,|x\rangle\,. \tag{8.2.2}$$

Orákulum aplikované na všetky prvky (okrem víťaza) bude vracať pôvodný prvok. Orákulum aplikované na víťaza mapuje víťaza na $-|x\rangle$, čo znamená, že bude zmenené znamienko amplitúdy víťaza (inak povedané fáza sa zmení o 180 stupňov). Pravdepodobnosť výberu jednotlivých stavov zostala rovnaká (pravdepodobnosť víťaza vypočítane ako $\left(-\frac{1}{\sqrt{n}}\right)^2$) [30].



Obr. 8.7: Stavy systému po aplikácií kvantového orákula

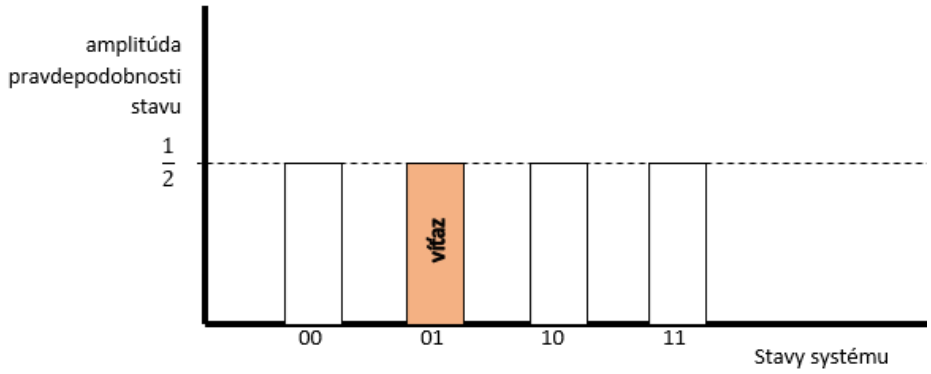
Zosilnenie amplitúdy

Zosilnenie amplitúdy predstavuje kľúčový blok Groverovho aplgoritmu. Amplitúdu zosilníme preklopením každej amplitúdy stavu okolo priemernej amplitúdy. Ak preklopíme stavy $|00\rangle$, $|10\rangle$, $|11\rangle$ okolo priemeru dostávame amplitúdu $\left(1-\frac{4}{n}\right)\frac{1}{\sqrt{n}}$), ak preklopíme okolo priemeru víťaza dostávame amplitúdu $\frac{3}{\sqrt{n}}$. Pravdepodobnosť výberu všetkých prvkov bude menšia ako pravdepodobnosť výberu víťaza. Opakované použitie kvantového orákula zvyšuje amplitúdu víťaza a tým aj pravdepodobnosť nájdenia víťazného prvku [30].

8.2.2 Samostatná úloha

Postup samostatnej úlohy môžeme zhrnúť do nasledujúcich bodov:

1) Spustenie simulátoru kvantového počítača.
2) Inicializácia počiatočného stavu.
3) Implementácia kvantového orákula.
4) Amplitude amplification = zosilnenie amplitúdy.



Obr. 8.8: Stavy systému po zosilnení amplitúdy

5) Meranie výsledného stavu.

ad 1) Spustenie simulátoru kvantového počítača

Pre potreby tohto cvičenia využijeme kvantový simulátor Quirk dostupný na adrese https://algassert.com/quirk. K tomu aby ste si vyskúšali ako funguje orákulum a overili jeho funkčnosť preskočte na bod 3. Bod 2 vykonajte po tom, čo sa zoznámite s orákulom.

ad 2) Inicializácia počiatočného stavu 4-qubitového systému

Všetky vstupy systému nastavíme na stav $|0\rangle$. Následne všetky stavy uveďte do superpozície (bloky umiestnite pred už vytvorené orákulum).

ad 3) Implementácia kvantového 4-qubitového orákula

a) Kvantové orákulum pre víťazný prvok otáča fázu o 180° a ostatné prvky necháva bezo zmeny. Vyberte vhodnú operáciu (ďalej bude na ňu odkazované ako na vybranú operáciu), ktorá túto funkciu bude reprezentovať (napr.X-operácia, Z-operácia, Hadamard, Y-operácia) – zatiaľ ju do obvodu neumiestňujte.

ad 3) Implementácia kvantového 4-qubitového orákula

a) Kvantové orákulum pre víťazný prvok otáča fázu o 180° a ostatné prvky necháva bezo zmeny. Vyberte vhodnú operáciu (ďalej bude na ňu odkazované ako na vybranú operáciu), ktorá túto funkciu bude reprezentovať (napr.X-operácia, Z-operácia, Hadamard, Y-operácia) – zatiaľ ju do obvodu neumiestňujte.

b) Pre štvorqubitový systém existuje celkom 16 možných konfigurácií orákula (stav $|0000\rangle$, $|0001\rangle$, $|0010\rangle$ atď.). K tomu aby sme nemuseli pre každý stav vytvárať

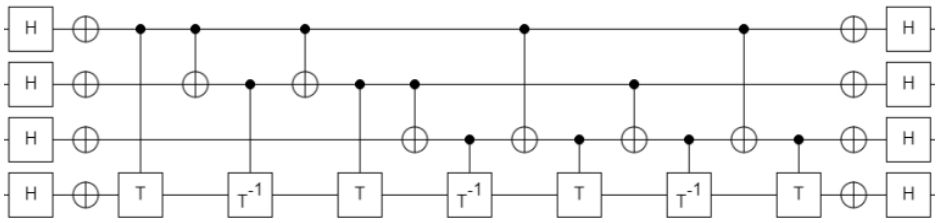
nové orákulum, ale len pozmenili jeho nastavenie, použijeme nasledujúce nastavenie obvodu:

- Vybranú operáciu umiestnene na qubit D.
- Pred vybranú operáciu vložte X-operáciu na ten qubit, ktorý chcete interpretovať ako Off (pre stav $|0000\rangle$ chceme všetky qubity interpretovať ako Off).
- Za vybranú operáciu vložte X-operáciu na ten qubit, ktorý chcete interpretovať ako Off (pre stav $|0000\rangle$ chceme všetky qubity interpretovať ako Off).
- Vybranú operáciu zviažte s qubitmi A,B,C tak, aby kontrolovala, či sa daný qubit nachádza v stave On.

Obvod by mal fungovať tak, že pokiaľ budú všetky vstupy v stave Off bude pravdepodobnosť stavu $|0000\rangle$ 1 a fáza bude 180°. Pokiaľ by sme chceli otočiť fázu stavu $|0001\rangle$ odstránime X-operácie na qubite A, a vstup A nastavíme na On. Vyskúšajte si rôzne kombinácie výstupných stavov (napr. $|0011\rangle$, $|0111\rangle$). Pozor: v ďalšom postupe (po zosilnení amplitúdy) sa zmena stavov bude vykonávať výhradne pomocou odstránenia X-operácií (vstupné qubity budú ponechané v Off stave). Pokračujte k bodu 2.

ad 4) Zosilnenie amplitúdy

Zosilnenie amplitúdy je možné vytvoriť pomocou tzv. Groverovho operátora. Jeho schéma je na obrázku 8.9. Operátor vložte za orákulum.



Obr. 8.9: Groverov operátor

ad 5) Meranie výsledného stavu

Vyskúšajte vyhľadať stavy $|0101\rangle$, $|0101\rangle$. Aká je pravdepodobnosť stavov, ktoré nemajú byť vyhľadané? Aká je ich fáza?

9 Záver

Táto práca sa zaoberala popisom vybraných kvantových logických funkcií, algoritmov potrebných pre kryptoanalýzu (vrátane ich dopadu na bezpečnosť) a tiež popisu kvantovo bezpečných schém. Ďalšia časť práce je tvorená návrhom aplikácie demonštrujúcej kvantové výpočty a kryptoanalytické algoritmy vrátane vytvorenia dvoch samostatných laboratórnych úloh.

Prvá až piata kapitola bola venovaná kvantovým počítačom od matematických základov až po súčasný stav vývoja. V prvej kapitole boli predstavené matematické princípy počítania s kvantovými stavmi a to najmä z pohľadu kvantového systému, ktorý tvorí pravdepodobnostný systém nad komplexnými číslami. Nasledujúca kapitola na prvú priamo nadväzuje, a to tak, že uvádza príklady kvantových operácií, s ktorými súčasné kvantové počítače umožňujú pracovať. Tretia kapitola sa zaoberala fyzikálnou implementáciou qubitu, pričom je bližšie predstavený Josephsonov efekt (využívaný kvantovým počítačom IBM Q) a tiež polarizácia fotónu či spin elektrónu. Štvrtá kapitola obsahuje demonštratívne vymenované javy ovplyvňujúce možnosti konštrukcie kvantového počítača. V piatej kapitole sú uvedené tri riešenia súčasného kvantového počítača – IBM Q, Intel (reálny kvantový počítač) a D-Wave (adiabatické kvantové výpočty).

Šiesta kapitola sa zaoberala kryptoanalytickými algoritmami, ktoré spôsobia zmeny v oblasti kryptografie v prípade skonštruovania dostatočne efektívneho kvantového počítača. Predovšetkým sa jedná o Shorov algoritmus, ktorý rieši faktorizačný problém a i problém diskrétneho logaritmu. Druhým dôležitým algoritmom je Groverov algoritmus umožňujúci zrýchlenie útokov hrubou silou.

Siedma kapitola tvorí úvod do postkvantovej kryptografie. Momentálny výskum je zameraný na štyri základne smery: kryptosystémy využívajúce hashe, kryptosystémy využívajúce teóriu kódovania, kryptosystémy využívajúce polynomiálne rovnice a kryptosystémy využívajúce mriežky. Z každej oblasti bola predstavená minimálne jedna schéma, ktorá zaručuje kvantovo bezpečnú kryptografiu.

Posledná časť práce bola zameraná na vytvorenie webovo založenej aplikácie, ktorá predstavuje nástroj pre výuku. Výkladová časť bola doplnená animáciami, ktoré demonštrujú spôsob činnosti vybraných algoritmov. Web obsahuje, okrem iného, dve laboratórne úlohy – jedna je zameraná na zoznámenie študenta s kvantovými operáciami, so spôsobom vytvorenia kvantového obvodu pomocou jednotlivých operácií a na vysvetlenie javov ako je superpozícia, či kvantové previazanie. Úloha je rozdelená do piatich čiastkových úloh, pričom každá úloha pracuje s iným

druhom operácie. Druhá úloha popisuje postup vytvorenia Groverovho algoritmu na kvantovom simulátore Quirk.

Literatúra

[1] JONES, J. A. a Dieter JAKSCH. *Quantum information, computation and communication*. New York: Cambridge University Press, 2012. ISBN 978-1-107-01446-6.

[2] AARONSON, Scott. Quantum information and the Brain. In: *Videolectures*[online]. 16.1.2013 [cit. 2018-11-06]. Dostupné z: <http://videolectures.net/nips2012_aaronson_quantum_information/>.

[3] GIDNEY, Craig. Grover's Quantum Search Algorithm. *Twisted Oak*[online]. 5.3.2013 [cit. 2018-11-06]. Dostupné z: <http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm>.

[4] Richard Feynman on Quantum Mechanics Part 1 - Photons Corpuscles of Light. In: *Youtube* [online]. 15.10.2011 [cit. 2018-11-26]. Dostupné z: <http://youtu.be/dR8SAFRBmcU>.

[5] KYRILLIDIS. Introduction to quantum computing: Bloch sphere. *Tasos posts* [online]. [cit. 2019-04-27]. Dostupné z: <http://akyrillidis.github.io/notes/quant_post_7>.

[6] ARUNA, A. G., K. H. VANI, C. SATHYA a R. SOWNDARYA MEENA. A Study on Reversible Logic Gates of Quantum Computing. *International Journal of Computer Science and Information Technologies.* 2016, **1**(Vol. 7), 427-432. ISSN 0975-9646.

[7] ROELL, Jason. Demystifying Quantum Gates – One Qubit at a Time. *TowardsDataScience* [online]. [cit. 2019-04-27]. Dostupné z: <https://towardsdatascience.com/demystifying-quantum-gates-one-qubit-at-a-time-54404ed80640>.

[8] KULHÁNEK, Petr. *Aldebaran bulletin: Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie.* AGA a Štefánikova hvězdárna v Praze, 2017, **15**(38) [cit. 2018-11-25]. ISSN 1214-1674. Dostupné z: <https://www.aldebaran.cz/bulletin/2017_38_ibq.php>.

[9] KULHÁNEK, Petr. *Aldebaran Bulletin: Týdeník věnovaný aktualitám a novinkám z fyziky a astronomie.* [online]. Praha: AGA a Štefánikova hvězdárna v Praze, 2017, **15**(37) [cit. 2018-12-12]. ISSN 1214-1674. Dostupné z:<https://www.aldebaran.cz/bulletin/2017_37_kvp.php>.

[10] The DiVincenzo criteria. *TUDelft* [online]. [cit. 2018-11-26]. Dostupné z: <https://ocw.tudelft.nl/wp-content/uploads/QIP3_divincenzo_criteria.pdf>.

[11] Experience Documentation: Beginners Guide. *IBM Q* [online]. 2017 [cit. 2018-11-06]. Dostupné z URL: <https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=beginners-guide&page=000-FAQ_for_Beginners~2F001-FAQ_for_Beginners>

[12] AARONSON, Scott. *Quantum computing since Democritus.* Cambridge: Cambridge University Press, 2013. ISBN 0521199565.

[13] SHOR, Peter W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing* [online]. 1997, 26(5), 1484-1509 [cit. 2018-10-21]. DOI: 10.1137/S0097539795293172. ISSN 0097-5397. Dostupné z URL:: http://epubs.siam.org/doi/10.1137/S0097539795293172

[14] JOHN A. SMOLIN, GRAEME SMITH a ALEXANDER VARGO. Oversimplifying quantum factoring. *Nature*[online]. Nature Publishing Group, 2013, 499(7457), 163 [cit. 2018-11-25]. DOI: 10.1038/nature12290. ISSN 0028-0836.

[15] Mersenne factorization factory. *In: Advances in Cryptology – ASIACRYPT*. 2015 [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, 9453 [cit. 2018-11-25]. DOI: 10.1007/978-3-662-48800-3. ISBN 978-3-662-48799-0.

[16] DASH, Avinash, Deepankar SARMAH, Bikash K. BEHERA a Prasanta K. PANIGRAHI. *Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer*. [online]. 2018 [cit. 2018-11-25].

[17] IBM Q Network. *IBM Q* [online]. [cit. 2018-10-19]. Dostupné z URL: <https://www.research.ibm.com/ibm-q/network/>.

[18] What is quantum computing?: Brief history of quantum computing.*IBM Q* [online]. [cit. 2018-10-19]. Dostupné z URL: <https://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/>.

[19] IBM Builds Its Most Powerful Universal Quantum Computing Processors: IBM Doubles Compute Power for IBM Q Commercial Systems with New Processor Developers, Researchers and Programmers Execute more than 300,000 Quantum Experiments on IBM Cloud. *IBM* [online]. 2017-05-17 [cit. 2018-10-19].

Dostupné z URL:
<hhttps://www-03.ibm.com/press/us/en/pressrelease/52403.wss>.

[20] *Quantum devices and simulators* [online]. [cit. 2018-10-19]. Dostupné z URL: <https://www.research.ibm.com/ibm-q/technology/devices/>.

[21] KNIGHT, Will. IBM Raises the Bar with a 50-Qubit Quantum Computer. *MIT Technology Review* [online]. 2017-10-10 [cit. 2019-03-17]. Dostupné z: <https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/>.

https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/

[22] HSU, Jeremy. CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy. *IEEE spectrum* [online].2018-1-9 [cit. 2019-03-17]. Dostupné z: <https://spectrum.ieee.org/tech-talk/computing/hardware/intels-49qubit-chip-aims-for-quantum-supremacy>.

[23] Intel´s 49-qubit processor. *Newsroom-intel* [online]. 2018 [cit. 2019-03-17]. Dostupné z: <https://newsroom.intel.com/wp-content/uploads/sites/11/2018/05/49-qubit-processor-tangle-lake-infographic.jpg>.

[24] Intel Labs is producing quantum processors in Oregon and doing system-level engineering that targets production-level quantum computing within ten years. *Reinventing Data Processing with Quantum Computing [online]*. [cit. 2019-03-17]. Dostupné z: <https://www.intel.com/content/www/us/en/research/quantum-computing.html>

[25] The D-Wave 2000Q Quantum Computer: Technology Overview. *D-Wave Systems Inc.*[online]. [cit. 2018-11-06]. Dostupné z: <https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral_1029F.pdf>.

[26] RØNNOW, Troels F., Zhihui WANG, Joshua JOB, et al. *Defining and detecting quantum speedup* [online]. 2014, 345(6195) [cit. 2018-11-25]. DOI: 10.1126/science.1252319. ISSN 00368075.

[27] BERNSTEIN, Daniel J., Johannes BUCHMANN a Erik DAHMÉN. *Post-quantum cryptography.* [online]. Berlin: Springer, c2009. [cit. 2018-11-19]. Dostupné z URL: <https://link.springer.com/chapter/10.1007%2F978-3-540-88702-7_1>.

[28] AARONSON, Scott. Shor, I'll do it. *Shtetl-Optimalized*. [online]. 24.7.2007 [cit. 2018-11-26]. Dostupné z: <http://algassert.com/post/1718>.

[29] CHILDS, Andrew. Quantum algorithms: LECTURE 2: The HSP and Shor's algorithm for discrete log. *University of Waterloo*. [online]. 2008 [cit. 2018-11-26]. Dostupné z: <https://www.math.uwaterloo.ca/~amchilds/teaching/w08/l02.pdf>.

[30] BERNSTEIN, Daniel J. Grover vs. McEliece. *Crypto*[online]. 7.4.2018 [cit. 2018-11-06]. Dostupné z: <http://cr.yp.to/codes/grovercode-20100303.pdf>.

[31] SCHWABE, Poter. *The transition to post-quantum cryptography* [online]. 2018 [cit. 2018-11-06]. Dostupné z: <https://cryptojedi.org/peter/data/nancy-20180219.pdf>

[32] BERNSTEIN, Daniel J. *Introduction to post-quantum cryptography* [online]. 2017 [cit. 2018-10-14]. Dostupné z URL: <https://eprint.iacr.org/2017/314.pdf>.

[33] BECKER, Georg. *Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis* [online]. 2018 [cit. 2018-11-06]. Dostupné z: <https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf>.Seminararbeit. Ruhr-Universität Bochum. Vedúci práce: Prof. Dr. Ing. Christof Paar.

[34] CHEN, Lily, et al. *Report on post-quantum cryptography.* [online]. US Department of Commerce, National Institute of Standards and Technology, 2016, [cit.2018-10-14]. Dostupné z URL: <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>.

[35] PETITCOLAS, Fabien A.P. Application of one-time Signatures: One-time signature basics. *Usenix*[online]. [cit. 2018-11-06]. Dostupné z: <https://www.usenix.org/legacy/publications/library/proceedings/ec98/full_papers/anderson/anderson_html/node14.html>.

[36] GREEN, Matthew. Hash-based Signatures: An illustrated Primer. *Cryptographyengineering*[online]. 7.4.2018 [cit. 2018-11-06]. Dostupné z: <https://blog.cryptographyengineering.com/2018/04/07/hash-based-signatures-an-illustrated-primer/>.

[37] How Log Proofs Work. *Certificate Transparency*[online]. [cit. 2018-11-06]. Dostupné z: <https://www.certificate-transparency.org/log-proofs-work>.

[38] BOLKEMA, Jessalyn, Heide GLUESING-LUERSSEN, Christine a. KELLEY, Kristin LAUTER, Beth MALMSKOG a Joachim ROSENTHAL. *Variations of the McEliece Cryptosystem*[online]. 2016 [cit. 2018-11-06]. Dostupné z: <https://www.certificate-transparency.org/log-proofs-work>.

[39] Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges. *Etsi*[online]. 2014 [cit. 2018-11-06]. Dostupné z: <https://portal.etsi.org/Portals/0/TBpages/QSC/Docs/Quantum_Safe_Whitepaper_1_0_0.pdf>.

[40] HOFFSTEIN, Joffrey. *NTRU-Sign: Digital Signatures Using the NTRU Lattice*[online]. [cit. 2018-11-06]. Dostupné z: <http://www.math.brown.edu/~jpipher/NTRUSign_RSA.pdf>.

[41] BERBAIN, Come. *QUAD: a Practical Stream Cipher with Provable Security*[online]. [cit. 2018-11-06]. Dostupné z: <https://iacr.org/archive/eurocrypt2006/40040110/40040110.pdf>.

Zoznam symbolov, veličín a skratiek

CVP	Closest Vector Problem
DSA	Digital Signature Algorithm
ECDSA	The Elliptic Curve Digital Signature Algorithm
MQ	Multivariate Quadratic
QPU	Qunatum Processing Unit
RSA	Rivest, Shamir, Adleman algoritmus
SVP	Shortest vector problem
XMSS	exTended Merkle Signature Scheme